School of Computing and Information Systems

"Forensic Computing: Exploring Paradoxes"

An investigation into challenges of digital evidence and implications for emerging responses to criminal, illegal and inappropriate on-line behaviours

by

Vlastimil Broucek
Grad.Dip.Sci.(IT), MSc(*Prague*)

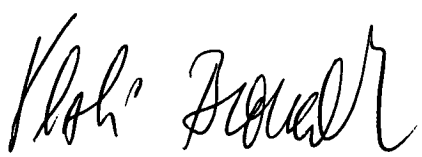
Submitted in fulfilment of the
requirements for the Degree of

Doctor of Philosophy

University of Tasmania (October 2009)

This dissertation contains no material which has been accepted for the award of any degree or diploma by the University or any other institution, except by way of background information and duly acknowledged in the thesis, and to the best of the candidate's knowledge and belief no material previously published or written by another person except where due acknowledgment is made in the text of the thesis.

This thesis may be made available for loan and limited copying in accordance with the *Copyright Act 1968.*



Vlastimil Broucek

26 October 2009

Abstract

This research thesis explores technical, legal and organisational challenges of digital evidence and the implications of their inter-relationships for responses to criminal, illegal and inappropriate on-line behaviours. From a forensic computing perspective the solutions to these challenges have tended to focus on discrete sets of technical, legal or organisational issues individually. Lack of understanding of the inter-relationships between these issues is inhibiting the development of integrated and coordinated solutions that can effectively balance requirements for the generation of legally admissible digital evidence, e-security and privacy. More significantly, this research highlights that the fragmented nature of these discrete approaches may be impairing the overall effectiveness of the responses developed.

The methodological framework underpinning this exploratory research adopts a subjective ontology and employs an interpretative epistemology. The research strategy involves the examination of three cases on technical, legal and organisational challenges of digital evidence respectively. Each case is analysed independently and the interpretation and discussion adopts a forensic computing perspective to interpret and discuss the inter-relationships across these areas and to explore the implications for digital evidence and the underlying problematic on-line behaviours. Case A examines the validity of quantitative data collected by running a network intrusion detection system (NIDS) SNORT on University network. Case B examines an Australian Federal Court case illustrating legal arguments applied to digital evidence, its discovery and presentation. Case C examines the Cyber Tools On-line Search for Evidence (CTOSE) project highlighting the difficulties of developing and implementing organisational level processes for digital evidence handling.

Analysis of Case A involves descriptive statistical analysis of network data and reveals significant problems with the validity and quality of the data. The results of the case analysis show that data collected by SNORT are not sufficient to track and trace the sources of the attacks. The analysis also

reveals that the data sets collected may be flawed, erroneous or already have been tampered with. Despite significant fine tuning, SNORT continued to generate numerous false positive alerts and/or wrongly identified sources of attacks. This case highlights that intrusion detection systems can play an important role in protecting information systems infrastructure, but to be effective they require the attention of highly trained security personnel/system administrators. These personnel also need to engage in regular monitoring and analysis of alerts and other log files, and to ensure regular updating of the rule sets used by these systems.

Analysis of Case B reveals the impact of legal misconceptualisations about the nature of digital systems on court decisions and on the generation of legal precedents that have potentially broader social implications. The results of the analysis reveal serious flaws in understanding amongst all participants in the case over the nature of digital evidence and how it should best be collected, analysed and presented. More broadly, the judgement also appears to have worrying implications for individual privacy and data protection.

Analysis of Case C highlights the practical challenges faced at the organisational level in the implementation of models and tools for digital evidence handling. The analysis highlights that models and tools that have been developed for handling digital evidence are by their very nature and complexity highly problematic to adopt and utilise in organisational settings. A key element that continues to inhibit their use is the lack of early and comprehensive end-user education. The results from this case highlight the critical need for organisations to have greater 'forensic readiness' for dealing with criminal, illegal or inappropriate on-line behaviours.

Interpretation and discussion of the analyses from the three cases adopts a forensic computing perspective and focuses on the nature of the inter-relationships between the issues identified in each case. From this perspective the discrete approaches adopted in each case limit an appreciation of the complex interplay between technical, legal and organisational factors, an

interplay that because of the nature of digital environments continues to have serious implications for each of these areas. More specifically, this interpretation and discussion reveals how and why this continued fragmentation of discrete approaches is impairing the overall effectiveness of the responses developed. A consequence of this is the lack of integrated and coordinated solutions that would effectively balance requirements for legally admissible digital evidence, effective e-security and data privacy.

At the broadest level, this research reveals these complex inter-relationships and confirms that they are likely to continue into the future as a result of uncoordinated research and development. The underlying paradoxes prevalent within the forensic computing domain result from the different concerns, interests and expectations of stakeholders and the nature and foci of research and development in each domain. This in turn ultimately leads to developments that are beneficial for improved performance in one area and at the same moment creates new challenges and inhibitors in another area. These circumstances have the on-going potential to trigger 'chain reactions' that ultimately may lead to more significant challenges than the problems they solve.

This research also reveals that the digital domain itself is also intimately related to the physical world where corroborative evidence and conventional investigative techniques have an equally important role to play. Ultimately, it is human behaviours that create these ongoing opportunities, challenges and risks. As a result, 'forensic readiness' also implies being able to grapple with moral, ethical and even political dimensions of these debates across the 'last mile' connection between digital behaviours and identifiable citizens.

In this context, forensic computing emerges as an approach that does not advocate for stronger laws, stricter technical systems and/or organisational protocols per se, but rather for the beginning of dialogue amongst these different requirements. In responding to the complex inter-relationships identified in this research, it is clear that solutions developed need to be aware

of their specific aims and objectives as well as the broader context, if we are to avoid the on-going 'band-aid' approaches.

This research thesis concludes that there is no easy solution to resolve the inter-relationships and paradoxes inherent within forensic computing issues. However, by recognising that these paradoxes exist, how they work and what their impacts are, measures can be developed to reduce their negative effects. In this regard, coordinated academic research is contributing to the emergence of cohesive and holistic approaches to understanding, implementing and evaluating the paradoxes within forensic computing.

Acknowledgments

This thesis is dedicated to my darling wife Paula, for her love, inspiration and never ending support and encouragement to finish this thesis even at times personally very difficult for her. I would have never finished this thesis without her never ending support and optimism.

I gratefully acknowledge the considerable support and assistance of my supervisors, Associate Professor Paul Turner, Professor Chris Keen and Dr Stephen Chau, all from University of Tasmania. I am particularly indebted to Associate Professor Paul Turner for his words of encouragement and support at various times throughout my research. His collegial approach, friendship, never ending optimism and reassurance to continue and finish this PhD research will always be remembered.

I would also like to acknowledge the valuable advice, many ideas and encouragement received from my colleagues at the European Institute of Computer Antivirus Research (EICAR), Digital Forensic Forum (DFF), Tasmanian Institute of Law Enforcement Studies (TILES) and many others. The list is too long to name them all.

Finally, I would like to thank the anonymous reviewers from the Boards of Editors/Reviewers of:

- The 5th Australian Security Research Symposium (Perth, Australia, 2001)
- The Journal Of Information Warfare (2001)
- The 2002 Information Resources Management Association International Conference (Seattle Washington, USA, 2002)
- 3rd International System Administration and Networking (SANE) Conference (Maastricht, The Netherlands, 2002)
- The 11th Annual EICAR Conference (Berlin, Germany, 2002)
- The Current Security Management & Ethical Issues of Information Technology. Hershey, PA 17033-1117, USA: IGP/INFOSCI/IRM Press (2003)

- The Cyber Tools On-line Search for Evidence (CTOSE) Conference (Namur, Belgium, 2003)
- The 12th Annual EICAR Conference (Copenhagen, Denmark, 2003)
- The 4th Australian Information Warfare and IT Security Conference (Adelaide, Australia, 2003)
- 1st Australian Computer, Network & Information Forensics Conference (Perth, Australia, 2003)
- The 13th Annual EICAR Conference (Luxembourg, Grand Duchy of Luxembourg, 2004)
- The International Review of Law, Computers & Technology (2004)
- The Computer Law & Security Report (2005)
- The 14th Annual EICAR Conference (Saint Julians, Malta, 2005)
- The International Scientific Journal of Computing (2005)
- The 15th Annual EICAR Conference (Hamburg, Germany 2006)
- The Journal in Computer Virology (France, 2006 and 2007)
- Digital Forensic Forum Conference (Prague, 2007)

who have provided valuable feedback on published papers relating to this PhD research.

Contents

List of Figures

List of Tables

1 Introduction

> *"Many criminal investigations will include computers at some point in the case. Murder and rape suspects may, through a search warrant, have their email and Internet activities analyzed to find evidence about their motives or hiding locations. Corporations investigate computers when an employee is suspected of unauthorized actions. Fraud investigations collect transaction history evidence from servers. It is therefore important that a process model for the digital investigation exists and that it easily interacts with the physical investigations that have long existed" (Carrier & Spafford, 2003).*

This research thesis explores technical, legal and organisational challenges of digital evidence and the implications of their inter-relationships for responses to criminal, illegal and inappropriate on-line behaviours.

This research involves an investigation of three independent cases that focus on the technical, legal and organisational challenges of digital evidence respectively. Each case is analysed independently and the interpretation and discussion explores the inter-relationships between the cases and their implications for ongoing responses to problematic on-line behaviours and the discipline of forensic computing.

This chapter provides a summary of the background to the thesis and identifies the primary research questions and research objectives. It also highlights the contribution that this research makes to the theory and practice of forensic computing and provides a summary of the other chapters in the thesis.

More specifically, the first part of this chapter provides a background to the area of forensic computing and highlights the adoption of a forensic computing perspective and how this re-positions both the problems and solutions experienced in relation to digital evidence in each of the three areas (technical, legal and organisational). This research reveals a lack of coordination amongst the discrete approaches that have been developed in each of the three areas to

address problematic on-line behaviours. More significantly, the forensic computing perspective adopted highlights how the nature of digital evidence and these problematic behaviours create inter-relationships that challenge the very solutions developed in each discrete area.

The second part of this chapter describes the research problem and presents the primary research questions and research objectives. In addition, this section also describes the scope of the research.

The third part of this chapter presents the justification for this research and summarises the contributions made at the substantive, methodological and theoretical levels.

The final part of this chapter provides a summary outline of the thesis structure and its chapters.

1.1 Background

In exploring the technical, legal and organisational challenges of digital evidence and the implications of their inter-relationships for responses to criminal, illegal and inappropriate on-line behaviours, this thesis adopts a forensic computing perspective. Forensic computing has become the focus of considerable academic and industry attention in the last ten years and has usefully been defined by Broucek and Turner (2006) as:

> "*the processes or procedures involving monitoring, collection, analysis and presentation of digital evidence as part of 'a priori' and/or 'post-mortem' investigations of criminal, illegal or other inappropriate on-line behaviours.*"

By adopting a forensic computing perspective, this research has been able to illuminate the inter-relationships amongst discrete approaches to the challenges of problematic on-line behaviours.

Forensic computing perspective is primarily concerned with generating a true and accurate picture of activities, timelines and events that have occurred on hosts, networks and in applications, to be in a position to validate whether criminal, illegal or other inappropriate on-line behaviours have occurred.

At one level, the forensic computing perspective is somewhat technical in its approach; however, it is this very perspective that enables the illumination of differences in approach, definitional ambiguities, and understandings amongst technical, legal and organisational experts. By highlighting the persistence of these differences amongst experts from different disciplines, it becomes possible to account for the continued lack of coherence in responses to the challenges faced.

More broadly, forensic computing can be seen as being similar to forensic medicine, forensic psychology and other 'forensic' disciplines. However, of course, the nature of the subject matter that forensic computing deals with – digital data and corroborative information – makes it very different. For example, while the subject matter of a discipline like forensic medicine is physically tangible, i.e. a human body or part thereof, the subject matter of forensic computing tends to be more intangible in its nature. It is difficult to 'touch' data travelling over the Internet or through wireless networks and although it is possible to touch a physical computer, it is again very difficult to inspect, observe or 'touch' the actual data stored on that computer. Additionally, the data in computers and other digital communication devices and networks are in the form of binary code rather than in human readable form.

Forensic computing is also often incorrectly understood as computer forensics. However, computer forensics is primarily focused on the usage of computing technology to support conventional human forensic work. In this context, computers are used to help in other forensic disciplines – for matching DNA, fingerprints and many other time consuming tasks. Huge amounts of data are

stored in databases and retrieved by computers as part of forensic examinations.

This thesis concentrates on forensic computing or as it is increasingly being referred to by the terms e-forensics and digital forensics.

The next three subsections provide a very brief introduction to some of the challenges being faced and responses being developed to problematic on-line behaviours within technical, legal and organisational areas.

1.1.1 Technical Area

Criminal, illegal and inappropriate on-line behaviours are most often considered to be problems for computer security, military intelligence and cyber-policing experts. Problematic on-line behaviours that involve computer misuse (e.g. malware, hacking) and/or are assisted by computer (e.g. internet paedophilia, fraud) have led to an explosion of industry, government and academic research, development and commercial activity (Denning, 1999; Etter, 2000a, 2000b, 2000c).

As a result, developments in the technical area of computer security, for example antivirus software, continue to occur rapidly both in the commercial and open source arenas. It is, however, important to recognise that the drivers for new developments vary between researchers and commercial operators. Indeed, it has been argued that despite numerous new products emerging on to the market, most commercial vendors are reactive to problems rather than proactive (Broucek & Turner, 2005b, 2006).

Additionally, developments in these technical areas tend to focus exclusively on improving technical capabilities of the tools such that questions around digital evidence are marginalised or ignored.

1.1.2 Legal Area

In contrast to the speed of development in the technical area, developments in the legal area remain relatively slow and tradition bound. While national and international frameworks do exist to address some of the challenges posed by digital technologies and the Internet, the practice of law within the court systems exhibit considerable variation.

Aside from problems of applicable law or the technological neutrality of particular legal codes, problems exist with legal professionals understanding of digital technology when making analogies with pre-existing case law. The digital domain poses significant conceptual challenges to notions of chain of evidence, chain of custody, original versus copy and legal admissibility.

Additionally, responses in these legal areas have often ignored how changes in one area of digital information law have direct or indirect consequences for the balance of rights in another area of information law. For example, it has been argued that strengthening digital intellectual property rights can have negative consequences for personal privacy and information access (Samuelson, 2002).

1.1.3 Organisational Area

With developments in electronic commerce, organisations have been quick to recognise the commercial opportunities provided by the Internet. However, most have become aware of the risks posed by criminal, illegal or inappropriate on-line behaviours by their employees, customers or criminals. In particular, organisations remain concerned about fraud, defamation and loss of reputation, financial loss and the loss of a competitive edge.

In response to the above mentioned issues, organisations have developed policies and procedures to safeguard themselves. However, it can be seen that a lack of understanding of the nature of digital information and users' on-line behaviours often means these approaches compound the very problems that they are trying to solve (Broucek & Turner, 2003a).

Additionally, regardless of the effectiveness of organisational approaches, there remains a strong tendency to 'pull the plug' when problems are detected rather than to engage in a systematic investigation, collection and analysis of digital evidence of the on-line behaviours that have occurred (Leyden, 2000; Maher, 2001; Microsoft, 2000; Microsoft UK website Hacked - VIGILANTe Statement," 2001; Mitnick, 2000; Rohde, 2000).

1.2 The Research Problem

As indicated above, digital technologies and the Internet open up potential risks from problematic on-line behaviours that have become the focus of interest for technical, legal and organisational researchers and practitioners. While each set of responses face difficult challenges to overcome, it is only by adopting a forensic computing perspective that the implications of a lack of coordination amongst these responses can be investigated.

Forensic computing requires a multidisciplinary approach (Broucek & Turner, 2001a, 2001b) and itself continues to be the subject of much debate concerning definitions, models and approaches. Broucek and Turner (2001b) presented an initial taxonomy of the field and this was later developed and extended (Hannan, Turner, & Broucek, 2003). Other models and definitions have been developed by other players, for example by First Digital Forensic Research Workshop (Palmer, 2001) and by EU funded project CTOSE (CTOSE, 2003; Urry & Mitchison, 2003). These models and definitions also reflect the ongoing debates inherent within the root disciplines that contribute to its multi-disciplinary nature.

Most significantly, a forensic computing perspective allows for an examination of each specific area and its response to problematic on-line behaviours as well as providing a conceptual framework within which to explore the implications of their inter-relationships. The lack of coordination and fragmentation that appears evident is caused by the fact that each area is grappling with its own problems, issues and challenges. The researchers and practitioners in each of the areas are attempting to address these challenges and ultimately make their

area 'better'. Unfortunately, by making improvements in one area, another area may be negatively affected and suffer significantly, thereby diminishing the overall effectiveness of the responses (Broucek & Turner, 2005a, 2005b).

This research thesis aims to explore the problems and challenges in each area, the responses being developed in each area and the implications of the inter-relationships across these areas for digital evidence and the underlying problematic on-line behaviours.

1.2.1 The Research Questions

To address the research problem identified above, two research questions were formulated:

Research Question 1: What are the key technical, legal and organisational challenges of digital evidence?

Research Question 2: What inter-relationships exist between technical, legal and organisational approaches and what implications do these have for the responses being developed?

1.2.2 The Research Objectives

A review of the research literature presented in Chapter 2 reveals that there has been limited academic research into technical, legal and organisational challenges of digital evidence and/or the implications of their inter-relationships for responses to criminal, illegal and inappropriate on-line behaviours. There are large numbers of publications and ongoing research projects within each area (technical, legal, organisational); however, to date there appears to be limited research investigating questions of digital evidence or inter-relationships amongst the responses being developed. In answering the research questions above, this thesis has the following research objectives:

- Identify the key technical, legal and organisational challenges of digital evidence;

- Determine the inter-relationships between the technical, legal and organisational approaches;
- Understand the key tensions and contradictions within and between each area in relation to digital evidence and problematic on-line behaviours;
- Explore the implications of these inter-relationships for emerging responses to criminal, illegal and inappropriate on-line behaviours;
- Identify potential solutions balancing the interests of privacy of the individual, security for the network and the demands of the courts for legally admissible evidence.

1.2.3 The Research Scope

To answer the research questions and satisfy the research objectives detailed above, the scope of this research involves the conduct of three independent case studies, each analysing challenges of digital evidence within technical, legal and organisational areas respectively. Following independent analysis of each case this research adopts a forensic computing perspective to interpret and discuss their inter-relationships and to explore the implications for emerging responses to criminal, illegal and inappropriate on-line behaviours.

In the technical area, Case A concentrates on an examination of data collected by the open source Intrusion Detection System (IDS) called SNORT. This IDS was at the time of conducting the experiment considered to be the best IDS available in the world. Case A focuses on an Intrusion Detection System partly because of the strong public disagreement between two leading experts (Sommer (1998b) and Stephenson (2000a, 2000b)) about the usability of IDS for collection of digital evidence (Broucek & Turner, 2003c).

In the legal area, Case B concentrates on an examination of an Australian legal case - Sony Music Entertainment (Australia) Limited v University of Tasmania heard in the Federal Court of Australia. This case was selected mainly because it involved the University of Tasmania (the host institution of the researcher) making access to detailed information on the case more available (Broucek, Turner, & Frings, 2005).

In the organisational area, Case C concentrates on organisational experience of a European methodology developed for digital evidence acquisition (CTOSE). This case was selected because of an opportunity to participate as a collaborating researcher in the European project developing the methodology (Hannan, Turner, et al., 2003).

1.3 Justification for the Research

The information society is based on computers and networked communication technology. The Internet is increasingly accessible and is being adopted and utilised by all sectors of society. For example, in Australia, "*the rate of access has quadrupled in recent years, from 16% of Australian households in 1998 to 64% in 2006–07*" (Australian Bureau of Statistics, 2008).

This increased use of network technologies creates both greater opportunities and greater risks to individuals, organisations, governments and society as a whole. Unfortunately, some users engage in problematic on-line behaviours.

These criminal, illegal or inappropriate on-line behaviours can be deliberate or accidental and have the potential to do more than simply challenge computer security. They also have implications for the privacy of individuals and for organisational and legal responses to them and the acquisition of evidence of these behaviours.

At the substantive level, this thesis contributes three case studies specifically focused on the challenges of the digital evidence. By adopting a forensic computing perspective this research also illuminates the range of inter-relationships that exist across the cases and the implications that these pose for the way in which potential future solutions may be developed that more effectively balance a range of requirements.

At the methodological level, this thesis illustrates the utility of the forensic computing perspective for revealing complex inter-relationships across individual areas of knowledge that are not immediately evident to experts within those specific areas.

At the theoretical level, this thesis contributes to an improved understanding of complex nature of digital evidence and on-line behaviours as well as pointing a way forward through the inherent paradoxes that exist within the digital domain and its links with the 'real' world.

Accordingly, this thesis aims to contribute to an enhanced understanding of the challenges faced and to the future development of more holistic responses that more effectively balance the interests of privacy of the individual, security for the network and the demands of the courts for legally admissible evidence.

1.4 Summary of other Chapters

Chapter 2 presents a review of existing literature relevant to the research. The chapter presents literature relating to:

- Information society and risk of computer misuse;
- Definitions and models of forensic computing;
- Intrusion detection systems;
- Information systems and technology issues;
- Legal aspects and dimensions; and
- Organisational challenges and issues.

Finally, the chapter presents literature on emerging trends that has been published subsequent to the completion of case study analyses.

The number of publications relevant to this research has significantly increased since 2001 when this research started. As a result, it is acknowledged that the literature review identifies only the key trends and directions across the three domains (technical, legal, organisational) with the aim of highlighting potential intersections that are then explored through the case studies.

Chapter 3 presents the research method used to conduct this research. The methodological framework underpinning this exploratory research adopts a subjective ontology and employs an interpretative epistemology. The research strategy involves the examination of three cases on technical, legal and

organisational challenges of digital evidence respectively. Each case is analysed independently. The interpretation and discussion adopts a forensic computing perspective to interpret and discuss the inter-relationships across these areas and to explore the implications for digital evidence and the underlying problematic on-line behaviours. Case A examines the validity of quantitative data collected by running a network intrusion detection system (NIDS) SNORT on a university network. Case B examines an Australian Federal Court case illustrating legal arguments applied to digital evidence, its discovery and presentation. Case C examines the Cyber Tools On-line Search for Evidence (CTOSE) project highlighting the difficulties of developing and implementing organisational level processes for digital evidence handling.

Chapter 4 provides analysis of Case A. The analysis involves descriptive statistical analysis of network data and reveals problems with the validity and quality of the data. The results of the analysis show that data collected by SNORT are not sufficient to track and trace the sources of the attacks. The analysis also reveals that the data sets collected may be flawed, erroneous or already have been tampered with. Despite significant fine tuning, SNORT continued to generate numerous false positive alerts and/or wrongly identified sources of attacks. This case highlights that intrusion detection systems can play an important role in protecting information systems infrastructure, but to be effective they require the attention of highly trained security personnel/system administrators. These personnel also need to engage in regular monitoring and analysis of alerts and other log files, and to ensure regular updating of the rule sets used by these systems.

Chapter 5 provides analysis of Case B. The analysis of the case reveals the impact of legal misconceptualisations about the nature of digital systems on court decisions and on the generation of legal precedents that have potentially broader social implications. The results of the analysis reveal serious flaws in understanding amongst all participants in the case over the nature of digital evidence and how it should best be collected, analysed and presented. More

broadly, the judgement also appears to have worrying implications for individual privacy and data protection.

Chapter 6 provides analysis of Case C. The analysis highlights the practical challenges faced at the organisational level in the implementation of models and tools for digital evidence handling. The analysis highlights that models and tools that have been developed for handling digital evidence are by their very nature and complexity highly problematic to adopt and utilise in organisational settings. A key element that continues to inhibit their use is the lack of early and comprehensive end-user education. The results from Case C highlight the critical need for organisations to have greater 'forensic readiness' for dealing with criminal, illegal or inappropriate on-line behaviours.

Chapter 7 provides an interpretation and discussion of the complete data set. The interpretation of the data brings together analyses conducted in Chapters four to six.

The interpretation and discussion of the analyses from the three cases adopts a forensic computing perspective and focuses on the nature of the inter-relationships between the issues identified in each case. From this perspective the discrete approaches adopted in each case limit an appreciation of the complex interplay between technical, legal and organisational factors. This interplay continues to have serious implications for each of these areas because of the nature of digital environments. More specifically this interpretation and discussion reveals how and why this continued fragmentation of discrete approaches is impairing the overall effectiveness of the responses developed. A consequence of this is the lack of integrated and coordinated solutions that would effectively balance requirements for legally admissible digital evidence, effective e-security and data privacy.

Chapter 8 provides the conclusions of this research. A synthesis of the main findings of the research is presented, along with a brief discussion of the limitations of the study, and an outline for future research work.

2 Literature Review

"The persistence of data, however, is remarkable. Contrary to the popular belief that it's hard to recover information, it's actually starting to appear that it's very hard to remove something even if you want to. The unrm/lazarus combination is a fine, if a bit unsettling, trash can analyzer. And while the results can be spotty for simple single file 'undeletion', robbing graves for fun and profit can be a lucrative venture for an aspiring forensic analyst. Indeed, when testing this software on a disk that had been used for some time on a Windows 95 machine, then reinstalled to be a firewall using Solaris, and finally converted to be a Linux system, files and data from the prior two installations were clearly visible. Now that's data persistence!"
(Farmer, 2001)

2.1 Introduction

This chapter provides a review of literature relevant to this research. There exist substantial bodies of academic and commercial literature of relevance to this research. In the discipline of computer science research relating to computer security, antivirus software, cyber crime and cyber terrorism have increased significantly over the last ten years. The organisational and legal aspects of computer security as well as research exploring broader social and privacy impacts of the information society have also increased dramatically. As a result, it is acknowledged that the literature review identifies only the key trends and directions across the three domains (technical, legal, organisational) with the aim of highlighting potential intersections that are then explored through the case studies[1].

[1]Given the rapid developments in each of the bodies of knowledge relevant to this thesis, it is noted that some of the web links and technical tools referred to have been superseded and as of March 2009 a number were found not to be 'live'.

The first section provides information about the information society and the influence of the growing availability of the Internet for the growth in risks of computer misuse. It also provides a classification of computer misuse that has been used through this research.

The second section discusses various definitions and models of forensic computing as they have been developed by various researchers and forums.

The third section provides an overview of Intrusion Detection Systems and research on them current at the time of the conduct of Case A data collection and analysis.

The fourth section introduces key technological issues faced in information systems and computer security, and in particular the use of log files as a source of forensic data.

The fifth section discusses legal aspects and dimensions of forensic computing, including privacy concerns.

The sixth section introduces literature relevant to a consideration of key organisational challenges and issues with networked computer systems and the Internet.

The final section of this chapter presents literature on emerging trends that has been published subsequent to the completion of case study analyses.

2.2 Information Society and Risks of Computer Misuse

The information society refers to the idea of a society in which information plays a significant economic, political and cultural role. This idea also acknowledges the central role of information technology in such a society, and this transformation is leading to the replacement of the 'industrial society'. Terms such as knowledge society, information revolution and network society are frequently used interchangeably with the term information society (Castells, 2000).

Unsurprisingly, debates continue on the idea of the 'information society' and there remains no universally accepted definition. Fortunately, most authors do agree that this social transformation started in the 1970s and that it continues to change the ways in which contemporary societies work. There is a large amount of literature discussing the evolution and definition of the information society, for example by Richta (1977), Webster (1997) and Touraine (1988).

One useful broad definition comes from a report by European Union High-Level Expert Group, defining the Information Society as

> *"The society that is currently being put in place, where low-cost information and data storage and transmission technologies are in general use. The generalisation of information and data use is being accompanied by organisational, commercial, social and legal innovations that will profoundly change life both in the world of work and in society generally." (European Commission, 1997)*

Increased access to the Internet and to networked technologies has brought enormous opportunities for businesses, governments and citizens. On the other hand it also brings an increase in challenges and risks faced by the society. Debates about ownership, control, censorship and commercialisation of the Internet are becoming more and more prevalent (Heller, 2008; Wu, 2003; Zittrain, 2008). There are reasonable fears that if the network becomes too regulated and/or privately owned, the growth of it and the benefits of it to the society will be slowed down. Indeed, the 'gridlock economy paradox' as defined by Heller (2008) argues, the Internet can even be stopped. Authors like Wu (2003) and Zittrain (2008) argue that developments related to 'Internet network neutrality' may even lead to the 'death' of the Internet. This threat to the 'neutrality of the web' is so strong, that Internet Freedom Preservation Act Bill 2009 ("Internet Freedom Preservation Act," 2009) has been introduced in the House of Representatives on 31 July 2009. This is a third attempt for such legislation in the USA since 2005.

2.2.1 Growth of Computer Misuse

The most visible risk to the information society, however, is the rapid growth in computer misuse and e-crime that has resulted from the increased number of ways that individuals and groups can engage in criminal, illegal or inappropriate on-line behaviours (Denning, 1999; Etter, 2000a, 2000b, 2000c). It is difficult to obtain accurate and reliable data on the scale and cost of these activities due to the fact that companies chose not to publish such data to protect their interests. As an example, even as early as 2004, the survey from the Australian Computer Emergency Response Team (Australian Computer Emergency Response Team, 2004) estimated that computer attacks on the integrity, availability and confidentiality of networks and systems in Australia had increased to over $15 million in 2004 up 20% on 2003. This survey at the time also indicated that:

- Malware in the form of viruses, worms or trojans was the most common form of attack and the cause of the greatest financial losses. The majority of attacks were also sourced externally;
- The second most significant cause of financial losses were the theft of laptops and the abuse/misuse of computer network access or resources;
- The two most significant factors contributing to susceptibility to harmful electronic attacks were un-patched or unprotected software vulnerabilities and inadequate staff training and education in security practices.

While the upward trajectory of these figures is alarming in itself, it is likely that the current reality is considerably more serious due to the incidence of non-reporting (AusCERT suggests this may be as high as 75% of incidences) and/or non-detection (Etter, 2001). Unsurprisingly, the increasing incidence of e-crime and computer misuse has stimulated strong demand from public and private sector organisations for effective ways to respond. This demand has contributed to a diverse range of research and development into technical, organisational and legal aspects of computer misuse and e-crime.

At one level, the rapid developments occurring in each of these areas are mostly laudable and exciting, but there is now increasing recognition that the development of truly effective defensive and offensive solutions will require the integration of insights from each area. While the complexity of specific issues within each area partly explains the limited collaboration that has occurred to date between researchers, it is also clear that it is inhibiting the development of the integrated solutions and skills that will be required to effectively balance needs for network security, individual privacy and the generation of legally admissible digital evidence. More significantly, there is growing proof to suggest that a consequence of this 'riding furiously in all directions' without an awareness of how developments in one area interact with developments in another is actually impairing the overall effectiveness of the responses developed (Broucek & Turner, 2001a, 2001b; Broucek, et al., 2005; Hannan, Frings, Broucek, & Turner, 2003; Hannan, Turner, et al., 2003).

2.2.2 Classification of Computer Misuse

To be able to examine the inter-relationships of technical, organisational and legal responses to computer misuse and e-crime it is useful to firstly classify the types of the misuse and the nature and seriousness of associated behaviours.

While existing mechanisms for addressing conventional societal misconduct (including law enforcement, education and security) remain relevant in the digital domain, there are also unique challenges for the investigation of behaviours in cyber-space because of the numerous ways in which individuals and/or groups can use digital technologies to engage in criminal, illegal or inappropriate on-line behaviour. As with conventional investigations when a computer incident occurs there is a need to assess its extent and effect and to rectify any damage caused. However, there may also be the need to gather evidence to identify the perpetrators and their 'intent' as a basis for future responses. From a forensic computing perspective it is these digital evidence acquisition activities, the 'last mile' connection (Hannan & Turner, 2004)

between them and an identifiable perpetrator, questions over the chain of custody, the determination of where the e-crime/misuse has occurred and questions on applicable law and legal admissibility that pose the most challenging technical, organisational and legal questions.

In responding to these questions, an important component in ensuring the effective identification of the type of forensic evidence required and the best methods for its collection, analysis and presentation is the ability to classify the type of misconduct as early in the investigation as possible. In this regard, one classification approach based upon the identification of behaviours cross-referenced with types of misuse was developed by Broucek and Turner (2001a, 2001b) and explored in Hannan, Frings et al (2003). The behaviours are identified as: criminal, illegal or inappropriate. This reflects the varying levels of seriousness of any behaviour committed and the likely penalties that will result from any investigations (i.e. criminal prosecution, civil proceedings or organisational censure or dismissal). The types of computer misuse identified are divided into two categories:

- Computer misuse, and
- Computer supported (or aided, assisted) misuse.

The first category involves misuses that

> *"encompass all offences against the confidentiality, integrity and availability (CIA) of computer data and systems. Examples include illegal access to computer systems or malicious code-writing" (Rathmell & Valeri, 2003).*

In this case the evidence collected will need to prove that the activities were intended to result in a specific criminal, illegal or inappropriate result.

The second category is defined as crimes that

> *"are 'traditional crimes' that can be, or have been, committed utilising other means of perpetration which are now being, or are capable of*

being, executed via the Internet, computer-related venue (e-mail, newsgroups, internal networks) or other technological computing advancement. For example, intellectual property rights infringement (e.g. digital music and software piracy) and payment system frauds (e.g. credit card fraud via the Internet" (Rathmell & Valeri, 2003).

In this case the evidence collected will need to prove that the delivery was intentional and the content of the transmission was not altered from the sender to the recipient.

Another way to classify computer misuse is to adopt matrix of behaviours and types of computer misuse developed by Hannan, Frings, et al. (2003). In this approach, criminal, illegal and inappropriate behaviours are ranked on their severity and then two types of computer misuse are defined.

Type 1 is defined as

> *"misuse arising from the generation, collection, storage, manipulation or distribution of data that itself constitutes a criminal, illegal or inappropriate behaviour" (Hannan, Frings, et al., 2003)*

and Type 2 is defined as

> *"misuse arising from the actions of the user deploying digital devices" (Hannan, Frings, et al., 2003).*

By putting the behaviours and types of computer misuse together, the Matrix is created as displayed in Figure 1.

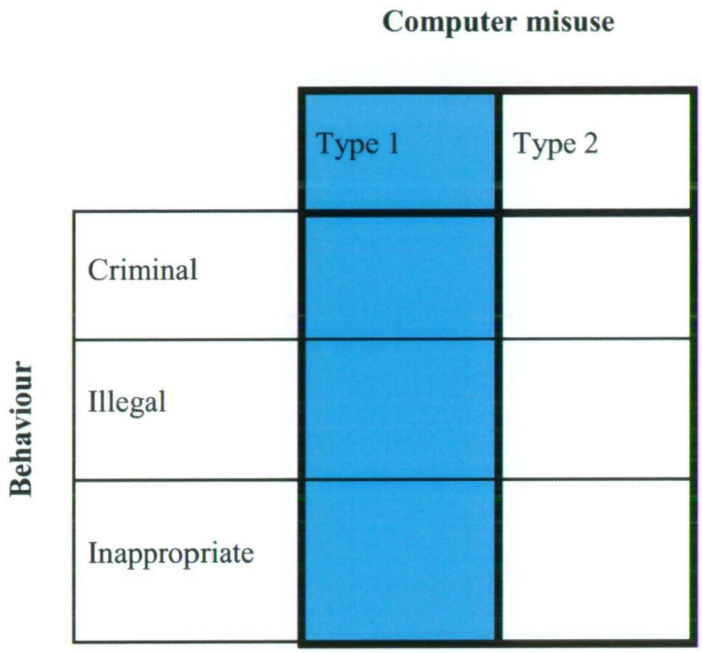


Figure 1: Matrix of behaviours and types of computer misuse (adapted from Hannan, Frings, et al., 2003)

2.3 Definitions and Models of Forensic Computing

Before exploring definitions and models of forensic computing, it is useful to explore approaches to the definition of digital evidence. Unfortunately, the same definitional problems that appear to hamper development in forensic computing also apply to the definition of digital evidence (DE).

Digital evidence has been previously defined by several authors. Casey (Casey, 2000) defines DE as

> *"any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator."*

The definition proposed by Standard Working Group on Digital Evidence (SWGDE) is narrower and emphasizes the legal dimension of digital evidence defining it as

> *"information of probative value stored or transmitted in digital form."(Scientific Working Group on Digital Evidence (SWGDE) & International Organization on Computer Evidence (IOCE), 2002)*

Other attempts at digital evidence definition have been made by Chisum (1999) who again has an inclusive definition of

> *"any data stored or transmitted using a computer that supports or refutes a theory on how an offence occurred or addresses critical elements of the offence such as intent or alibi".*

Interestingly, two of the most eminent researchers in the forensic computing domain have adopted Casey's broad definition in their work (Carrier & Spafford, 2003).

Attempts at defining digital evidence were also made in the European Cyber Tools On-line Search for Evidence (CTOSE) project (CTOSE, 2003; Urry & Mitchison, 2003). This project is examined in detail in Chapter 6. This definitional ambiguity appears to relate to the technical, organisational or legal backgrounds of the authors and again highlights the challenges facing forensic computing resulting from its multi-disciplinary roots.

Academic research publications on forensic computing and its definition first began to appear at the end of 1990s (Bates, 1997, 1998). From the beginning, definitional difficulties were obvious as illustrated by the two different approaches adopted by McKemmish (1999) and Farmer and Venema (1999), respectively.

McKemmish (1999) defines forensic computing as

> *"the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable"*

and then continues by defining four key elements of forensic computing as:

- *"identification of digital evidence,*
- *preservation of digital evidence,*
- *analysis of digital evidence, and*
- *presentation of digital evidence."*

This clearly demonstrates the author's law enforcement background and clear interest in legally acceptable evidence.

Dan Farmer & Wietse Venema, two well known computer security experts, started running forensic computing classes around the same time and for that purpose defined forensic computing as

> *"gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system" (Farmer & Venema, 1999).*

This definition completely ignores any mention of the legal acceptability of the evidence produced. This is in spite of the fact that forensic computing by the nature of the word 'forensic' implies "*used in or connected with a court of law*" (Hanks, 1991).

Subsequent to these definitions, Palmer (2001) provided a much broader definition containing implied criticism of both previous approaches because of their overly narrow focus (legal or technical).

> *"the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Palmer, 2001).*

The fact that several different definitions emerged at about the same time illustrates the 'youth' of forensic computing and the need for a conceptual framework to reduce confusion and frustration for researchers attempting to explore forensic computing and the inter-disciplinary dimensions of issues related to identification, collection and analysis of computer evidence.

Broucek and Turner (2001a, 2001b) contributed to the development of this conceptual framework by assessing the range of topics and viewpoints intersecting in the research space central to the developing discipline of forensic computing. They developed a preliminary taxonomy for forensic computing and identified four major constituent disciplines – computer science, law, information systems and social science. Subsequent work expanded this list to include law enforcement and the basic taxonomy of the forensic computing domain is illustrated in Figure 2 (Broucek & Turner, 2001a, 2001b; Hannan, Frings, et al., 2003; Hannan, Turner, et al., 2003).

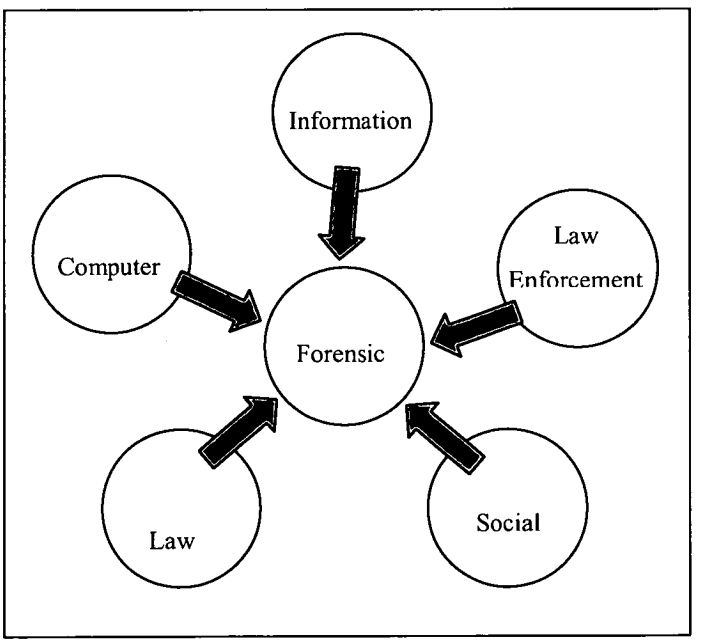


Figure 2: Forensic Computing Domain

Based on this research work, Broucek and Turner developed their own definition of forensic computing as follows.

> *"Processes or procedures involving monitoring, collection, analysis and presentation of digital evidence as part of 'a priori' and/or 'post-mortem' investigations of criminal, illegal or other inappropriate on-line behaviours" (Broucek & Turner, 2006).*

This definition encompasses the fact that forensic computing is and will be used not only in criminal cases, but also in civil cases and other avenues where digital evidence will be required. It also encompasses fact that it is not necessarily enough to conduct 'post mortem' analysis of existing data, but also 'a priori' data will be needed to provide evidence.

It should however be noted that this taxonomy and definition are by no means the only attempts to define the domain. Indeed, as a result of collaborative work at the First Digital Forensic Workshop (DFRWS) in 2001, an entirely different approach based not on constitute disciplines but rather specific fields of computer forensic activity led to the development of an alternative model referred to as the 'Nucleus of Digital Forensic Research'. This model is displayed in Figure 3.

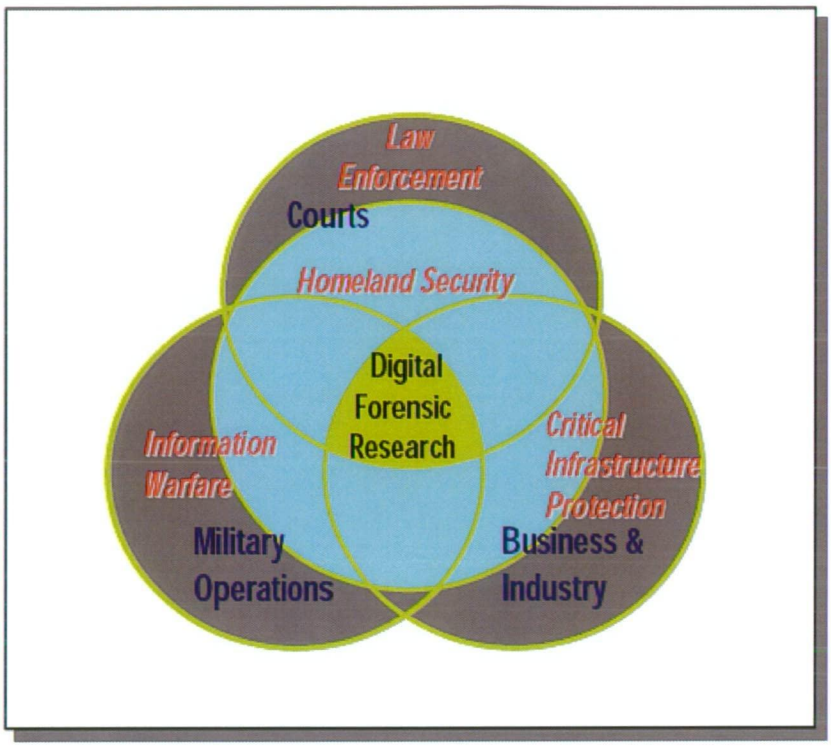


Figure 3: Nucleus of Digital Forensic Research (from Palmer, 2001)

Interestingly, both the 'taxonomy' and 'nucleus' frameworks emphasize the need to stimulate cooperation and collaboration amongst the various disciplines and fields concerned with forensic computing issues. The same urgency to support interaction and collaboration has also been suggested by Spafford (cited in Palmer, 2001, p. 7). Spafford argues that it is necessary to:

- Abandon current 'band aid approaches' to forensics. The same approach was and still is often observed in the security world – the security elements are added into the existing or new systems, instead of designing the systems with security already built in;
- Know exactly how much information and what type of it needs to be collected for further analysis in particular circumstances; and
- Understand social aspects of 'the game'.

Spafford concludes that in the forensic computing domain

> *"All aspects of the problem are essential. Therefore, it is imperative that each collaborates with the other. Researchers, investigators, legislators, and jurists must all work toward a central goal. This requires constant discussion within groups that have representation from all essential parties" (Palmer, 2001, p. 8).*

The significance of these remarks is that despite their apparent conformity and agreement, an academic analysis of the work arising from, for example the First Digital Forensic Research Workshop, reveals the markedly different aims, goals and objectives underpinning the approaches of different domain experts.

As the presentations of the main speakers at the DFRWS workshop illustrate (i.e. Eugene Spafford representing academic research and government, Charles Boeckman representing DOD Operations, Chet Hosmer representing Commercial Tools development, David Baker representing Critical Infrastructure Protection and John Hoyt representing Law Enforcement), the different underlying positions can be summarised as follows:

- Law enforcement agencies appear primarily interested in gathering evidence that can later be used for prosecution. It is worth pointing out that such evidence must follow rules of evidence established by particular jurisdictions to maintain evidential integrity (chain of custody) and that the digital evidence should form a part of the 'whole case' such that non-technical elements are also taken into account;
- Business requirements are more or less driven by economic pressures of remaining viable and competitive;
- Academics are interested in exact, scientific methods and data and in the advancement of new knowledge; and
- Military and Information Warfare Operations are mainly interested in what is referred to as Defensive Information Operations (DIO). DIO represents a multi-disciplinary approach to protecting digital systems. It includes Communication, Computer, Information and Operational Security as well as Physical Security, and other tactics used in active systems protection.

The main differentiation of defence operation requirements from those in law enforcement is willingness of DIO to sacrifice absolute and/or even measurable accuracy for quickness in order to serve a mission's timeline. The result of DIO is research conducted in defence operations concentrated mainly on three areas (Optimisation of data collection; minimisation of data corruption or destruction risks; Accommodation of operational time constraints).

Table 1, adapted and extended from Palmer (2001), clearly demonstrates that investigators from each area deploy different paradigms when approaching forensic computing and its analysis. Furthermore, it appears that researchers also attempt to do this in different environments and/or timeframes. Significantly, it is suggested that Law Enforcement is only interested in 'post-mortem' while all the other players tend to anticipate and try to take an action to thwart a possible threat even before it happens including such factors as financial cost, reputation, service availability.

Area	**Primary Objective**	**Secondary Objective**	**Environment - Time Frames**
Law Enforcement	Prosecution		After the act/post-mortem
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business and Industry	Availability of Services	Prosecution	Real Time
Academics	Advancement of Knowledge	Dissemination of Knowledge	Variable: Subject to Externalities

Table 1: Suitability Guidelines for Digital Forensic Research (adapted and extended from Palmer (2001)).

It is noticeable that the approach advocated by DFRWS can be directly linked to models that subsequently emerged focused on how to respond in conducting/implementing forensic computing investigations. Broadly these models can be divided into three categories Simple, Advanced and Complex. These are outlined below.

2.3.1 Simple Models

Arising directly out of the DFRWS was the development of 7 step linear model for the conduct of forensic computing investigations:

- Identification;
- Preservation;
- Collection;
- Examination;
- Analysis;
- Presentation; and
- Decision.

Reith, Carr, and Gunsch (2002) extended this model to nine steps and called it the Abstract Digital Forensic Model. The nine steps included are:

- Identification;
- Preparation;
- Approach Strategy;
- Preservation;
- Collection;
- Examination;
- Analysis;
- Presentation; and
- Returning Evidence.

These models concentrate on processing digital evidence. They do not identify flow in investigation, do not include issues like chain of custody and different requirements and needs of different groups of users as defined above and in (Palmer, 2001).

2.3.2 Advanced Models

Carrier & Spafford (2003) after analysis of several other models developed their 'Integrated Digital Investigation Process (IDIP)'. This model is based on crime scene theory for physical investigation. They argue that this investigation process has been refined over time through its use in thousands of investigations, and as such, is the most suitable model upon which to establish a model for digital investigations. As a result their model is based on the assumption that the computer should be treated as a separate crime scene to the extent that they use the analogy that the computer should be treated the same as a "*body at the murder scene*". (Carrier & Spafford, 2003, p. 18).

Carrier & Spafford's model has been extended by Baryamureeba & Tushabe (2004) with their Enhanced Digital Investigation Model (EDIP). The EDIP expands the IDIP to enable 'tracing back' in order to address the issues of digital investigations in networked and wireless environments. However, even with this enhanced model it is useful to consider how far the physical investigation analogy can be pushed given the challenges of incidental/multiple digital copies of any individual data element and the capacity of systems to 'tamper' with data during analysis (Broucek & Turner, 2005a, 2005b, 2006).

2.3.3 Complex Models

More complex model/framework has been developed by the European project Cyber Tools On-line Search for Evidence (CTOSE). Discussion of this model has been widely published and it has been examined in depth in the following papers (Broucek & Turner, 2004a; Broucek, et al., 2005; CTOSE, 2003; Leroux & Pérez Asinari, 2003; Sato, Broucek, & Turner, 2005; Urry & Mitchison, 2003). In summary, the CTOSE model was developed as a high level tool aimed to assist companies or other individuals/groups to respond correctly during the investigation and analysis of on-line behaviours in order to generate legally admissible evidence. The CTOSE approach was an attempt to develop an 'expert system' to guide users (for example, a company's security officer) in their preparations and responses to e-security incidents.

Importantly, the CTOSE approach aimed to bring to these organisations an overall benchmark against which to compare their own operations and procedures relating to evidence handling. The CTOSE framework offers an approach to integrate functionality across the whole spectrum of actors involved in the process of evidence handling. It appears that the CTOSE framework is the only framework to be comprehensive across the entire chain of evidence handling, across different types of organisations as well as across different countries. However, questions have now arisen over the extent to which this comprehensive approach has been adopted and used and what factors would stimulate more widespread implementation of the approach.

Finally, it is useful to review Ciardhuáin's (2004) 13 step model that integrates each step with a sequence of activities and information flows. To date, attempts have been made to validate this model through the conduct of interviews with police investigators and to deploy the model as part of genuine police computer forensic investigations. The thirteen steps of this model are:

- Awareness;
- Authorisation;
- Planning;
- Notification;
- Search for and identify evidence;
- Collection of evidence;
- Transport of evidence;
- Storage of evidence;
- Examination of evidence;
- Hypothesis;
- Presentation of hypothesis;
- Proof/Defence of hypothesis; and
- Dissemination of information.

In summary, it is evident that despite numerous attempts to model the forensic computing domain, definitional heterogeneity remains. It is evident that this

heterogeneity is at least partly due to the differing assumptions, aims, goals and objectives underpinning the approaches outlined above. Significantly, however, despite widespread recognition of the multi-dimensional nature of on-line behaviours and the challenges of understanding and responding to them, little progress has been made. Indeed, even where comprehensive frameworks have been developed the additional challenges of adoption and utilisation have emerged to limit the benefits, at the time when the incidents of computer misuse and e-crime continues to grow.

At one level, all the models examined above can usefully be classified as either 'organisational' or 'procedural'. As a consequence, these models do not explicitly consider actual practices, for example variations in the technical hardware and/or software, impact on the conduct and result of investigations. Similarly, these models also do not explicitly consider the impact of variability in the abilities and skills of investigators. In this regard, it is useful to note that within many jurisdictions it is sufficient to hold an undergraduate degree in computer science to enable an individual to act as expert e-forensic witness (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003).

These models tend to concentrate on the defence side of the problem and do not sufficiently describe the 'offensive or attack side' of the problem. These observations support the argument that there is the need for a more detailed conceptual/theoretical approach. One way might be to revisit information theories or adopt a purely mathematical model style of approach as advocated by Filiol (2006b).

While some readers may consider these issues merely of academic interest, this research highlights how this lack of coherence has directly inhibited awareness of the issues/challenges in the community, impaired the development and diffusion of specialised forensic computing skills and, most importantly, impacted directly on the effectiveness of responses to computer misuse and e-crime (Broucek & Turner, 2005b; Broucek, et al., 2005).

2.4 Information Systems and Technology Issues

> *"We cannot hope to protect our information infrastructure without a sustained commitment to the conduct of research -- both basic and applied -- and the development of new experts. The incredible growth of our society's deployment of computing has too often been conducted with concerns for speed or lowest cost rather than with concern for issues of safety, security, and reliability. Security cannot be easily or adequately added on after-the-fact and this greatly complicates our overall mission. The software and hardware being deployed today has been designed by individuals with little or no security training, using unsafe methods, and then poorly tested. This is being added to the fault-ridden infrastructure already in place and operated by personnel with insufficient awareness of the risks. Therefore, none of us should be surprised if we continue to see a rise in break-ins, defacements, and viruses in the years to come." (Spafford, 2001)*

This section of the literature review aims to briefly introduce some of the key technical dimensions relating to digital data as it relates to computer security and forensic computing.

2.4.1 Distinguishing Computer Security from Forensic Computing

Patel and Ciardhuáin (2000) illustrated this distinction in their paper by noting that the distribution of child pornography is clearly illegal in most of the jurisdictions, however, it can be conducted without any breaches of computer security. Cases involving the distribution of child pornography highlight that the only technical requirements are properly setting up a digital distribution channel (for example web server). Consequently, there is no breach of computer security, but the activity is illegal and a subject of interest for forensic computing.

Another example illustrating a difference between the two fields has been discussed by Broucek and Turner (2001a, 2001b). Using their own experience

in network administration at the University of Tasmania they examined an instance of e-mail communications being used to send life threatening messages to a female student. Initially with only verbal threats, but later on with attached pictures and movies. At no time were any security measures breached. In this particular case the 'forensic' investigation was very easy because the offending e-mails were sent from a 'hotmail' account with the sender making no attempt to disguise his/her identity. Using simple UNIX commands (*nslookup*, *traceroute*) and looking into several log/auditing files) the offender was traced back to his/her dial-up point. This again illustrates key distinctions between computer security and forensic computing. Again, these repugnant activities were the focus of a forensic investigation but did not involve the breaching of any computer security.

Following Patel and Ciardhuáin (2000) the most important differences between computer security and forensic computing can be illustrated through answers to four questions about the foci of the two fields. These questions are: why, when, who and for whom?

- **Why** - Computer security is in place to protect against and to detect cyber-attacks. Forensic computing does not protect against the attacks. However, it is worth noting that as the field of forensic computing evolves, more proactive forensic tools may be developed that will blur this distinction. Currently, there are numerous computer security resources available to network and systems administrators to prevent and detect cyber-attacks. But these tools are not designed to provide data sets that are suitable for the generation of forensic evidence. This results in either insufficient data being collected or the data being potentially unreliable. Both raise problems for collection and presentation of forensic evidence.
- **When** - Computer security is ideally conducted in real time while forensic computing is primarily conducted 'post mortem' i.e. after the occurrence of criminal, illegal or other inappropriate behaviour. However, as noted in previous point this distinction will be again narrowed with the evolution of more proactive forensic computing tools.

- **Who** - Computer security is primarily conducted by computer specialists. Forensic computing can be conducted by a wide range of professionals, many of whom do not have specialised computer security skills. Of course, ideally forensic computing specialists should be trained in all the disciplines that were identified earlier. Indeed, there has already been at least one senior US government official proposing the establishment of training facilities and funding to develop these types of professionals (Reno, 1996). The same issues were identified during Police Commissioners' Conference on Electronic Crime Strategy held in March 2001 in Australia (Australasian Centre For Policing Research, 2001).
- **For whom** - Computer security is usually subject to minimal presentation requirements. Also if it is presented this is usually to a highly technically literate audience. However, the results of forensic investigation are always presented to non-IT/IS audiences and frequently in the context of legal proceedings.

To conclude this topic, Table 2 shows distinctive differences between computer security and forensic computing

Computer Security	**Forensic Computing**
Protects the system against attack	Does not protect the system against attack
Usually in real time	Conducted 'Post mortem'
Conducted by computer specialists	Can be conducted by computer specialists, but often this is not the case
Restricted environment for presentation of developments, issues	Evidence is nearly always presented to non-IT/IS personnel
Can be bypassed by trusted individuals/users	Integrity of the evidence is most important

Table 2: Computer Security versus Forensic Computing

Aside from these overt differences, there is a major problem with existing computer security approaches that is only revealed by adopting a forensic

computing perspective. This problem emerges from the fact that computer security measures can be, and often are bypassed by 'trusted users'. This fact points to a broader and age-old question of 'who polices the police?'. With root user[2] access, it is possible to do almost anything on the systems including modifying or deleting log files and disabling system and security processes.

Following Farmer (2001), deleted files can be relatively easy to restore; However, the processes used makes problematic the legal validity of the subsequent data set (Farmer, 2001). From a forensic computing perspective the lack of existing checks and balances on users with root access raises a fundamental problem concerning the integrity of computer data to be used as evidence.

Despite these differences computer security expertise is a central plank for developing the appropriate skill sets for the field of forensic computing. The ability to identify, track, trace and analyse log files is central to forensic investigations where digital evidence is main source of data. However, the forensic computing perspective moves beyond these technical skills to develop sensitivity towards questions over the admissibility of evidence and legal validity of particular data sets. This is particularly the case during the analysis of log files where 'dirtying of the data' or 'acontextual' presentation may significantly alter the meaning of the evidence.

2.4.2 Intrusion Detection Systems (IDS)

Intrusion detection systems have been suggested by some authors as suitable tools for collecting network data for legal evidence (Stephenson, 2000a, 2000b). On the other hand, there have been strong arguments against the suitability of IDS for collection of forensic data (Sommer, 1998a, 1998b, 1999). Research has been conducted and attempt made to produce commercial

---

[2] 'root' user is historically username given to user with full access privileges on Unix/Linux systems. This term is generally used when talking about users with such privileges although in other systems the actual username might be different – administrator, admin etc.

products. For example Patel and Ciardhuáin (2000) advocated the need for 'network black box'.

As the dangers of hacking and cyber-warfare for network security become a reality, the need to be able to generate legally admissible evidence of criminal or other illegal on-line behaviours has become increasingly important. While technical systems providing intrusion detection and network monitoring are constantly being improved, the security they provide is never absolute.

As a result, when assessing the value and nature of the data these systems produce, it becomes critical to be aware of a number of factors: these systems themselves are susceptible to attack and/or evasion (Arona, Bruschi, & Rosti, 1999; Handley, Paxson, & Kreibich, 2001; Ptacek & Newsham, 1998); these systems may only collect a partial data set; and, these data sets may themselves be flawed, erroneous or already have been tampered with (Broucek & Turner, 2002c). Additionally, the issue of privacy and data protection is emerging as a central debate in forensic computing research (Broucek & Turner, 2002c).

Although these advanced systems provide network administrators with the tools to treat some of the symptoms of such criminal, illegal and/or inappropriate on-line behaviours, they are not designed with the need to track, trace and generate legally admissible evidence about these behaviours. Additionally, there is a growing awareness that most computer security systems can easily be tainted and their evidence contaminated. As an example, it is well-known that there are numerous hacks for *wtmpx*, *utmpx* and other built-in system log files that are often used as a source of information on system events (Farmer & Venema, 1993) and papers have been published describing techniques used to avoid Intrusion Detection Systems (Handley, et al., 2001; Ptacek & Newsham, 1998).

IDS Classification

Bace & Mell (2001) classify IDS according to their three fundamental attributes – information source, analysis method and response. The first two attributes are particularly of relevance for forensic computing specialist.

Bace & Mell (2001) further recognise that three different sources of information are network, host and application. Laing (2000) introduces fourth source of information, TCP/IP stack. By accepting these different sources, it is possible to classify four different types of intrusion detection systems – network based IDS (NIDS), host based IDS (HIDS), application based IDS (AIDS) and stack based IDS (SIDS). Each of these systems has its own advantages and disadvantages that have been extensively discussed in Bace & Mell (2001) and in Laing (2000).

Based on the way how IDS analyse their data they are further classified as misuse detection and anomaly detection IDS. Misuse detection IDS use pattern matching principles. The data collected is constantly being matched against the typical patterns or 'fingerprints' of known attacks and vulnerabilities. The quality of these systems is determined not only by quality of their programming, but more significantly by quality of their pattern ('fingerprint') database. These systems cannot detect new attacks until the 'fingerprint' is available. Anomaly detection IDS are based on attempts to identify abnormal or unusual behaviour compared against the normal one. These systems can discover new attacks; however they are subject to high amount of false-positive alerts and to many more privacy issues that the signature based (Lundin, 2000; Lundin & Jonsson, 1999a, 1999b).

IDS Technical Issues for Forensic Computing

Several technical issues were identified in relation to intrusion detection systems and have been in detail discussed in Broucek & Turner (2002a, 2002c).

One of the major issues is that IDS may not be able to collect all the data that they are supposed to collect. Ever increasing speed of networking equipment requires further development in IDS. Better pattern matching algorithms and anomaly detection systems as well as data capturing methods need to be developed (Desai, 2002; Handley, et al., 2001; Kruegel & Toth, 2003). At the time of data collection for Case A, it was acknowledged that many then current systems had problems even at the speed of 100 Megabit per second.

Second issue arises from the fact that IDS can collect only partial, hence insufficient, information data. For example, in a case of NIDS, attacker is identified by IP address. Unfortunately this IP address is not enough to definitely identify attacking machine. Important research by Clayton (2000) suggests major limitations to traceability in legal proceedings. Even without legal limitations, IP addressing is clearly insufficient to identify actual host. Many sites and in particular ISPs employ dynamic DHCP to assign IP addressed to hosts. Each host is usually assigned different address during each connection. This can be overcome in a case of ISPs by using caller identification (CID – phone number) features and it is now a requirement in many countries that ISPs collect this CID. However, dynamic DHCP is used also at Universities etc and log files are not always maintained. Furthermore, even with CID and IP to MAC (even MAC can be spoofed) log files maintained, the attacker can be traced to the host only. The important question of a human being behind the attacking host remains again unsolved. This is mainly case where computers are shared and or on multi-user systems (e.g. UNIX and thin clients).

Third issue arises from the fact that IDS can themselves be susceptible to a variety of attacks (Ptacek & Newsham, 1998). Some authors even suggest (Handley, et al., 2001; Mell, Marks, & McLarnon, 2000) that the majority of intrusion detection systems are fundamentally flawed. This leads to the conclusion that data collected by IDS cannot be trusted. This argument is for example strongly supported by one of the confirmed flaws in SNORT IDS. This flaw opened SNORT to possible root compromise (see ESB-2003.0141 --

Snort Vulnerability Advisory -- [SNORT-2003-001] at http://www.auscert.org.au/render.html?it=2816) and made it vulnerable to data tampering by the intruder.

Based on these issues and work by Peter Sommer from the Computer Security Research Centre at London School of Economics and Political Sciences (Sommer, 1998b, 1999) in relation to famous "Rome Labs" attack (Christy, 1998), three major issues with IDS have to be examined:

- These systems may not be able to collect the data that they are designed to collect;
- Where data collection occurs, these systems may only provide a partial data set; and
- This data may itself be flawed, erroneous or have already been tampered with.

Finally, issues surrounding privacy principles and laws have to be examined as well. The debate about privacy highlights a curious paradox between requirements of privacy protection and increasing usage of communication tools that provide little or no privacy at all (e.g. e-mail systems using outdated and inherently insecure SMTP protocol (Klensin, 2001; Postel, 1982)). Unfortunately, the privacy issues are not related only to techniques for collecting data due to increasing need for constant monitoring and surveillance of computer networks. Age old question of 'who polices the police' emerges during the forensic examination of collected data. This data contain not only information about the case being investigated, but also about other individuals and other entities. Privacy concerns arising from constant surveillance are subject of research attention (Biskup & Flegel, 2000a, 2000b, 2000c; Kvarnström, Lundin, & Jonsson, 2000; Lundin, 2000; Lundin & Jonsson, 1999a; Sobirey, Fischer-Hübner, & Rannenberg, 1997), however, the results remain far from satisfactory both on technological and legal level.

In turning to examine the legal issues surrounding the use of IDS as a tool for collecting, collating and presenting forensic evidence, the 'Rome Labs' case

provides a good example of the strong differences of opinion that are evident amongst experts in the forensic computing field. The 'Rome Labs' Attack refers to a hacker attack against the Rome Air Development Center, Griffiss Air Force Base, New York, on March 28, 1994. This case is interesting also because the proceedings against one of the attackers were initiated in the United Kingdom.

Jim Christy (Christy, 1998) gave a report of this incident to the Senate Governmental Affairs Committee on May 22, 1996 that highlighted a number of key aspects of the case:

- The attack was only discovered five days after it occurred;
- The responsible commander at the Air Force Base allowed several systems to be kept open thereby allowing the forensic investigating team to trace the attackers; and
- Despite a thorough investigation by the Air Force Office of Special Investigations (OSI), numerous questions remained unanswered. These can be summarised as follows:
    - The identity and motivation of the second attacker, nicknamed Kuji;
    - The extent of the attack; and
    - The extent of the damage.

Peter Sommer from the Computer Research Security Centre at the London School of Economics was subsequently hired by defence lawyers in the UK to assess the quality of the evidence prepared by OSI. Sommer's assessment was significant in calling into question the quality of the evidence for presentation in a court of law. Subsequently published, Sommer (1998b, 1999) states that

"Almost every individual stream of evidence could be challenged".

Sommer goes on to discuss in detail several streams of evidence provided by OSI and as a result of his analysis provides a list of 11 points that should be followed in development of any new intrusion detection systems. Sommer's

work appears to be supported by the findings of the NSTAC Network Group Intrusion Detection Subgroup that in its December 1997 reports that:

- *"Current Intrusion Detection Systems are not designed to collect and protect the integrity of the type of information required to conduct law enforcement investigations".*
- *"There is a lack of guidance to employees as to how to respond to intrusions and capture the information required to conduct a law enforcement investigation..."*(cited in Sommer, 1998b, 1999)

This analysis also details a range of issues involved in using log files to derive evidence, particularly that they can be compromised prior and during collection of the evidence as well as during post-collection analysis.

Ultimately, this evidence was never tested in court because the defendant engaged in a plea-bargaining deal and pleaded guilty.

In contrast to Sommer's views, other authors have argued that IDS are indeed suitable for evidence acquisition (Stephenson, 2000a, 2000b) while others choose to ignore the legal aspects of evidence acquisition (Yuill, Wu, Gong, & Huang, 1999). In reality the opinions of these different authors are probably not as polarised as they might first appear. However, the disagreements do highlight that while IDS are among the best tools available to date for 'trying' to collect data that could be used in a prosecution, serious problems remain.

Since the Case A of this thesis examines SNORT that has been a forerunner in IDS area at the time of conducting the data collection for the case, it is beneficial to look at few more recent developments in IDS.

Developments by SourceFire (which basically evolved from a Network Intrusion Detection System (NIDS) based on SNORT) have produced a set of tools called the 3D approach of 'discover, determine and defend'.

This approach is represented in the Figure 4.

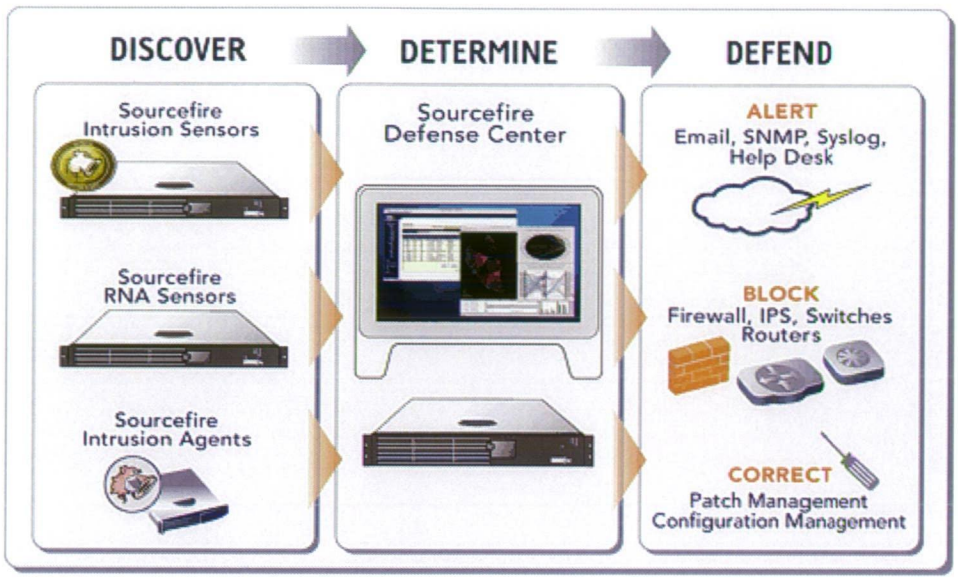


Figure 4: SourceFire's 3D approach (from http://www.sourcefire.com/products.html)

SourceFire argue that this approach is the "only comprehensive intelligent network defense system that unifies intrusion and vulnerability management technologies to provide customers with real-time network security". At the centre of the system is the SourceFire Defense Centre (SDC) that correlates data from the intrusion sensors and agents with the network intelligence provided by the RNA Sensors to prioritize the most critical security events prior to taking action in real-time. SourceFire claim that as a result of the 'high level of contextual intelligence' organisations can determine why changes occur, whether an attack poses a serious threat and how to best prioritize and shape the response. While the move from intrusion detection systems (IDS) to intrusion protection systems (IPS) offers some significant advantages in terms of security, it also raises numerous questions for the collection of digital evidence as these systems adopt an approach analogous to 'pulling the plug' that inhibits evidence acquisition activities (Broucek & Turner, 2001a, 2001b). Given the experience that few if any systems are perfect, it would seem sensible to ensure that more consideration is given to addressing circumstances where systems fail or prove unsuitable for responding to the challenges of illegal or inappropriate on-line behaviours.

Tripp's (2006) paper explores a novel approach for string matching for high speed Intrusion Detection Systems (IDS) applying finite state machine approach. He proposes the use of a set of finite state machines, each working on single byte of the data input. The paper illustrates Tripp's hardware design for a parallel string matching engine built for implementation in a Xilinx Field Programmable Gate Array and tested by simulation. In his next paper, Tripp (2007) continues with his hardware design for use within network intrusion detection systems. The paper describes an optimised finite state automata based hardware design for implementing high speed regular expression matching. The approach presented addresses the conventional memory problem faced by standard Field Programmable Gate Arrays (FPGA). Tripp explains how using an existing 'packed array' style of table based automata implementation can be enhanced by adding a form of input compression to group together characters.

Researchers from the Agent Technology Center, Department of Cybernetics, Czech Technical University in Prague and from the Institute of Computer Science, Masaryk University in Brno are working on a research prototype of a network intrusion detection system called CAMNEP (for more see http://agents.felk.cvut.cz/projects/camnep/). This intrusion detection system is based on an idea of collaboration of a community of detection agents, each of which embodies an existing anomaly detection model. The agents use extended trust modelling, a technique established in a multi-agent research field to improve the quality of classification provided by individual models. The agents then process un-sampled data acquired by dedicated high-performance NetFlow aggregation cards.

The researchers claim that their prototype provides among other benefits for:

- Improved effectiveness, i.e. less false positives/false negatives;
- High performance, the system is able to process 1Gb/sec of traffic on a single (multi-core) PC; and
- Minimal configuration upon deployment thanks to the self-adaptation features.

CAMNEP falls into the class of Network Behaviour Analysis systems, as it detects the attacks only using the statistics about the network traffic. According to the authors, together with the use of anomaly detection paradigm, this ensures that the system respects the privacy of the users (content of the network traffic is not examined), is robust with respect to traffic encryption and does not rely on a set of rules to describe the existing attacks, making it suitable for detection of zero-day attacks.

All these developments are targeted towards faster response to the new threats and improvement of the actual technology without considering other consequences.

2.4.3 Log Files as a Source of Forensic Data

Following Farmer and Venema (2000) the login session in Figure 5 reveals information recorded by three different login facilities of UNIX system. These are examined in turn to reveal problems in using this information in a forensic context.

```
May 25 10:12:46 spike telnetd[13626]: connect from hades.porcupine.org

      wietse   ttyp1   hades   Thu May 25 10:12-10:13 (00:00)

            hostname -   wietse   ttyp1   0.00 secs Thu May 25 10:12
            sed      -   wietse   ttyp1   0.00 secs Thu May 25 10:12
            stty     -   wietse   ttyp1   0.00 secs Thu May 25 10:12
            mesg     -   wietse   ttyp1   0.00 secs Thu May 25 10:12
            who      -   wietse   ttyp1   0.00 secs Thu May 25 10:12
            w        -   wietse   ttyp1   0.00 secs Thu May 25 10:12
            ps       -   wietse   ttyp1   0.00 secs Thu May 25 10:13
            ls       -   wietse   ttyp1   0.00 secs Thu May 25 10:13
            w        -   wietse   ttyp1   0.00 secs Thu May 25 10:13
            csh      -S  wietse   ttyp1   0.03 secs Thu May 25 10:12
            telnetd  -S  root     ----    0.00 secs Thu May 25 10:12
```

Figure 5: Adapted from Farmer and Venema (2000)

First, the entry from TCP wrappers log file (shown in the first line) shows that on May 25, at 10:12:46 local time, the machine spike received a telnet connection from the machine hades.porcupine.org. From a forensic perspective this is problematic because the TCP wrappers log files contain only information about the initial connection event. They do not provide a corresponding record for the end of the telnet connection. Therefore, for the forensic investigation, alternative sources of information have to be collected to substantiate the length of the connection.

Second, the output from UNIX *last* command (shown in the line starting with wietse) shows that the user wietse was logged in on port ttyp1 from host hades. This log apparently reveals that the login session lasted from 10:12 until 10:13 but does not provide details of how many seconds the session lasted; hence the log file shows 00:00 for the length of the session. From a forensic perspective this is problematic because there is a lack of detail as to the length of connection time. The system output (00:00) is clearly in conflict with the connection time start-end 10:12-10:13. It is also worth noting that this output uses only short name for the machine from which user wietse connected, while TCP wrappers used full name.

Third, output from the UNIX *lastcomm* command (lines starting hostname through to telnetd) shows the commands executed by the user wietse. Additionally, these lines show how much CPU time each command consumed in seconds, and at what time each command started (the last column of these lines). Significantly, *lastcomm* provides a record of the order in which each process is **terminated** (the column hostname through to telnetd). In this case the command interpreter (csh) and the telnet daemon (telnetd) appear at the end even though they were actually the first two processes started. From a forensic computing perspective this is problematic because there is no reliable and detailed record of the order in which the commands were actually run and for how long.

These technical weaknesses demonstrate the inadequacy of available login systems for forensic computing because the data provided is insufficiently complete, accurate or continuous. Additionally, as previously mentioned, any user with root access could easily modify these log files used by commands *last* and *lastcomm* to generate their respective outputs. Combined, these problems create major difficulties for the collection and presentation of digital evidence suitable for a court of law.

Increasingly there is an acknowledgement that computer security systems can easily be tainted and their evidence contaminated. There are many known hacks to fix *wtmpx*, *utmpx* and other log files often used as a source of information on system events (Farmer & Venema, 1993). In a series of articles Farmer and Venema (Farmer, 2000, 2001; Farmer & Venema, 2000; Venema, 2000a, 2000c) have dealt directly with these issues from a technical perspective. In a personal communication to the author, Venema indicated that forensic computing was still very immature and at the beginning of a steep learning curve (Venema, 2000b). However, beyond these technical approaches and given the 'Rome Labs' example there is a need for more consideration of the legal implications of manipulating log and audit files in terms of legal admissibility.

The issue of using audit logs as a source of evidence per se was in detail investigated by Allinson (2002) by analysing 11 cases from Queensland, Australia. She concluded that

> *"Legal and court proceedings do not yet appear to be at a level to fully assess the worth and acceptance of electronic evidence. This is demonstrated by the low level of cross-examination and the acceptance of material submitted at face value."*

While Allinson's conclusion is important, it is necessary to acknowledge the limited nature of her investigation to one state in Australia. It would be dangerous to make a general conclusion based on this investigation.

In terms of broad technical approaches, huge advances have been made in the last ten years in the ability of systems to detect intrusions, denial of services attacks and to improve user profiling and network monitoring. However, as AusCERT figures (Australian Computer Emergency Response Team, 2004) indicate it would be naïve to suggest that these approaches are wholly effective or even able to keep pace with the growing challenges of computer misuse and e-crime. Indeed, while these approaches may provide tools to address some of the major symptoms of computer misuse, problems remain in detecting, identifying and logging attacks. Additionally, as has been previously demonstrated through cases studies, many of the systems and tools developed within this approach have major limitations in terms of evidence acquisition capabilities (Broucek & Turner, 2002c, 2004b; Sommer, 1998a, 1998b, 1999). Significantly, it is also important to remain aware of the susceptibility of these systems and tools themselves to attack (Arona, et al., 1999; Handley, et al., 2001).

As the debates in the e-security and e-forensics literature indicate, responding to the challenges of computer misuse and e-crime has produced several streams of research and development including network survivability, self-healing networks, intrusion prevention/protection systems, anti malware systems and e-forensic investigation tools. Whilst various disagreements and debates continue within each of these streams of research, there appears to be an increasing awareness of the need to move from reactive to more proactive approaches. These new approaches appear to increasingly acknowledge that the conventional 'fortress model' of perimeter defence is no longer sufficient to address security on networks that have numerous entry points due to the range of devices (wired and wireless) and application service models now commonly deployed. For example, current developments in malware protection (antivirus software) are increasingly displaying a move away from signature-based (reactive) detection of malware exploits towards a more proactive approach of vulnerability protection through the deployment of behavioural-based engines. While this approach clearly offers assistance in protecting systems against new exploits without having to rely on their signature, there has been little

consideration of the implications of these systems for user privacy and the collection of digital evidence.

An example that illustrates another aspect of the interrelatedness of issues has occurred in the realm of anti-spam software. While many of these systems make valiant attempts to deal with the increasing problem of spam email, some of the solutions developed may be causing more harm than good. As the direct experience of one of the authors indicates, much anti-spam software is language specific and cannot cope with other languages, with the consequence that messages in these languages are frequently marked as SPAM. These types of problems with spam filtering may lead to the loss of messages (due to them being filtered to the junk mail folder and deleted without being examined). Additionally, given that some anti-spam software tools work on a principle of changing and or adding headers to e-mails to allow users to filter according to these headers, it remains unclear whether such modifications of e-mails might have legal implications, for example:

- If e-mail is used as an official document and a dispute arises, the originating e-mail will be different from e-mail delivered to recipient and thus may become invalid;
- If e-mail is going to be used as an evidence of criminal, illegal or other inappropriate activity, will such a modification render it inadmissible or invalid?

Even where digital data is potentially available there are still numerous technical challenges. For example, EnCase (currently the preferred e-forensic investigation software tool used by Australian law enforcement agencies) was the focus of considerable discussion in 2003. While it offered access to file systems other than those used by Microsoft Windows and DOS platforms, it was mainly oriented towards the MS Windows environment. At that time it could be run only on this platform and it was discussed in forensic circles in relation to producing different (potentially incorrect) hash values for disks imaged/investigated on two different platforms (http://groups-beta.google.com/

group/infosec-discuss/). This difference appeared to be the result of difficulties EnCase had in acquiring access to the HPA (Host Protected Area)[3] part of discs. Given the requirements in many jurisdictions for completeness of the disk image used for evidence, this raises interesting questions on admissibility. While other e-forensic software tools such as Brian Carrier's SleuthKit provide options for both MS Windows and Unix/Linux platforms, it too has some limitations, for example not supporting the ReiserFS file system used as a default on the commonly deployed SuSE (now Novell) Linux.

From a forensic computing perspective there is evidence that the various technical responses to the challenges of criminal, illegal or inappropriate on-line behaviours are increasingly raising problems for both the collection of data and its admissibility. However, it is clear that given our contemporary experience of computer security that we retain modest expectations of their capabilities. Therefore, even whilst arguing for the need for these systems developers to consider issues of evidence acquisition, there is a need following Broucek & Turner (2002c) to acknowledge that:

- These systems may not even be able to collect the data that they are designed to collect;
- Where data is collected it may only be a partial data set; and
- The data collected may itself be flawed, erroneous or have already been tampered.

More broadly, as technical responses become more 'proactive' they are raising increasing challenges for the conduct of forensic analysis and individual privacy. The nature of many of these new systems is also making the conduct of forensic analysis problematic because the methods that have to be used to access the evidentiary data end-up jeopardizing its legal admissibility. In

---

[3] HPA is defined as a reserved area for data storage outside the normal operating file system. This area is hidden from the operating system and the file system, and is normally used for specialized applications. Systems may wish to store configuration data or to save memory to the hard disk drive device in a location that the operating systems cannot change.

relation to privacy, the need for systems to collect data and also protect privacy is evidenced by work on pseudonymisation techniques for log files and intrusion detection systems (Biskup & Flegel, 2000a, 2000b, 2000c; Lundin, 2000).

Privacy concerns also emerge not just in relation to those individuals under investigation, but also to others whose activities are also part of the data sets being analysed. These knock-on effects involving privacy intrusion raise concerns about breaches of privacy and/or confidentiality without the knowledge or consent of the individual's concerned. With pro-active security measures, there are also privacy concerns arising from constant surveillance (Biskup & Flegel, 2000a, 2000b, 2000c; Kvarnström, et al., 2000; Lundin, 2000; Lundin & Jonsson, 1999a; Sobirey, et al., 1997). The emergence of anomaly based intrusion detection systems that rely on analysis of 'normal' work patterns poses a further threat to privacy as is witnessed by efforts to develop privacy protection through pseudonymisation approaches.

2.4.4 Anti-forensics

While several tools and solutions were previously developed as tools for enhancement of privacy and/or security, they can now be also considered as 'anti-forensic' tools i.e. tools and solutions that directly inhibit, hamper or at least limit accurate investigation of digital evidence.

First and foremost, as soon as any form of cryptography is introduced, an e-forensic investigation is significantly hampered. As previous work by Broucek and Turner (Broucek & Turner, 2003b, 2003c) observed and confirmed network based intrusion detection tools (NIDS) like SNORT can be rendered useless by simply using SSL for http protocol (https). Collected encrypted data has either no or minimal forensic value. The same applies for antivirus software. The majority of the detections are signature based and as such they are practically powerless against viruses that are distributed in encrypted form. As the Aldrich Ames Spy case illustrated (Reno, 1996), encrypted data files obtained as part of an investigation are basically useless as evidence. Clearly

for criminals, hackers and other individuals engaging in illegal or inappropriate behaviour, encryption provides protection.

Privacy enhancement tools such as PGP (Zimmerman, 1996, 2001) again decrease the ability of forensic investigators unless they have legal powers to recover encryption keys. This in turn reintroduces a key topic on the socio-political agenda at national and international levels about balancing privacy versus encryption control and recalls debates about Key Escrow (the old clipper debate) (Denning, 1997; Denning & Branstad, 1996; Reno, 1996).

Significantly, in the post 9/11 era there have been some anecdotally reported cases of 'self-incrimination' in relation to the use of encryption. Just the plain fact that someone starts using encrypted e-mails may increase suspicion on these individuals from authorities by raising the question 'why are these individuals exchanging encrypted e-mails?'.

Anti-forensic tools are increasingly the subject of debates at scientific and commercial conferences (for example, Annual Infosec World Conference and Expo; Black Hat Briefings). Increasingly, they are also becoming the subject of research and criticism.

Liu and Brown (2006) conducted a two hour session at the Infosec 2006 analysing various anti-forensic techniques and counter techniques from very simple ones that anyone can use, to complex and complicated approaches requiring tools and expert knowledge.

Geiger, (2005) evaluated seven commercial anti-forensic tools with surprising results:

> *"All the counter-forensic tools failed to eradicate some potentially sensitive information – either data specifically targeted for wiping by the user or records that contained information the tool was designed to eliminate. Some shortfalls were more serious than others. In one case, the tool failed to wipe, or overwrite, any of the files it deleted."*
> *(Geiger, 2005)*

While it is acknowledged that currently there is not widespread awareness of these tools, perhaps this is only a matter of time. It can also be anticipated that cyber-criminals are already aware of and using these commercially available tools. Some of these tools are actually built into existing software. For example, tools like CIPHER.EXE included in the standard distribution of WindowsXP, Vista and Windows 7 can significantly hinder forensic analysis.

While some recent research (for example, Geiger's evaluation (2005)) suggests that many of these anti-forensic tools are less effective than they claim to be and some actually do not work at all, their existence is illustrative of the nature of the problems faced and the need for integrated responses that balance the needs for security, privacy and legal admissibility.

2.5 Legal Aspects and Dimensions

> *"The world left the legal profession in the dust years ago. Attorneys are just coming to the realization that people have computers and have important information on them. I spend a good deal of time dragging attorneys kicking and screaming into the 20th century." (John Benson, e-discovery consultant, at Black Hat 2008)*

In contrast to the pace of change that has occurred in the development of the Internet and the information society, developments in the legal area continue to evolve relatively slowly and based on tradition bound approaches, processes and procedures. While national and international frameworks have emerged aimed at addressing some aspects of the challenges posed by digital technologies and the Internet, it is noticeable that the practice of law within national court systems continues to exhibit considerable variation.

Alongside problems of 'applicable law' because of the transnational nature of digital communications, and the relatively slow pace of development of international laws, regulations and procedures, it is clear that there are fundamental differences between scientific and legal proofs. While many lawyers recognise the need for technological neutrality in legal codes,

problems continue to exist with legal professionals understanding of digital technology when making analogies with pre-existing case law. The digital domain poses significant conceptual challenges to notions of chain of evidence, chain of custody, original versus copy and legal admissibility.

Additionally, the inter-relationships between responses in one legal area on another have often been ignored. This situation has become more significant with the expansion of the Internet and the information society as changes in one area of digital information law have direct or indirect consequences for the balance of rights in another area of information law. For example, it has been argued that strengthening digital intellectual property rights can have negative consequences for personal privacy and information access (Samuelson, 2002).

2.5.1 Risks and Challenges: the Law and Digital Data

In the 'information age' alongside exciting opportunities for activities such as e-business and e-learning, there is an awareness of the serious risks posed by malware, hacktivism and information-warfare. A fundamental cause of many of these risks is the variety of ways that individuals and/or groups can now utilise digital technologies to engage in criminal, illegal or other inappropriate on-line activities. While it can be assumed that much of this on-line behaviour continues to go undetected, when it is identified the need for evidence and proof becomes of paramount importance.

Although technical advances in the ability of systems to detect intrusions, denial of services attacks, other forms of attacks and to enhance network monitoring and maintenance are well documented and subject to constant research and development, their utility for the presentation of evidence in the court of law is rarely evaluated (McKemmish, 1999). Additionally, the issue of privacy and data protection is emerging as a central debate in forensic computing research (Broucek & Turner, 2002c).

Next section presents a short overview of three major legislative frameworks, namely EU Convention on Cybercrime (Council of Europe, 2001), Directive

on Privacy and Electronic Communication (European Parliament & Council of the European Union, 2002) and Cybersecurity Act of 2009 ("Cybersecurity Act of 2009," 2009).

Convention on Cybercrime (Council of Europe, 2001) had been four years in making. It was finally proclaimed in Budapest on 23 November 2001. This convention was first international treaty on cyber-crimes, with particular interest in dealing with crimes related to Intellectual Property (copyright), computer related fraud, child pornography and attacks against network security. One of the main objectives was to set up common criminal policies amongst the EU member countries as well as other countries and to establish grounds for mutual international cooperation.

The treaty is very conveniently divided into Articles and after the initial Article, Articles 2 to 10 clearly define the offense and what is expected from each party. There are following offences defined in these Articles:

- Article 2 – Illegal access
- Article 3 – Illegal interception
- Article 4 – Data interference
- Article 5 – System interference
- Article 6 – Misuse of devices
- Article 7 – Computer-related forgery
- Article 8 – Computer-related fraud
- Article 9 – Offences related to child pornography
- Article 10 – Offences related to infringements of copyright and related rights

The Convention also conveniently describes following procedural provisions:

- Article 15 – Conditions and safeguards
- Article 16 – Expedited preservation and partial disclosure of traffic data
- Article 19 – Search and seizure of stored computer data
- Article 20 – Real time collection of traffic data

Chapter three stipulates principles of international cooperation. It deals with general principles of mutual cooperation, extradition, mutual assistance and spontaneous information.

Importantly, Article 28 deals in detail with principles of confidentiality and limitation on use.

The Convention entered force on 1 July 2004 after gaining minimal number of required signatures and ratifications. Unfortunately, process of signing and ratifying has been very slow and not exactly satisfactory. As of 15 April 2009 the Convention was signed by 42 EU member countries and 4 non-members. It has been ratified only by 4 member countries and one non-member country (USA).

Directive on Privacy and Electronic Communication (European Parliament & Council of the European Union, 2002) was adopted by European Parliament on 12 July 2002. This directive deals with questions and issues surrounding privacy in electronic communication. The directive provides valuable definitions for terms like 'user', 'traffic data', 'consent', 'value added services', 'electronic mail' and other in Article 2.

In the Article 4, the directive stipulates need to provide security of the services and in a case of particular risks to the security, provide information of such risk to the subscribers.

Article 5, provides for confidentiality of communication. It specifically requests adoption of national laws prohibiting listening, tapping, storage or other kinds of surveillance and interception without consent of the user, unless legally authorised, as provided for in Article 15.

In relation to the data retention and other uses, the directive stipulates need for anonymisation of the data when no longer needed and that retention is possible only for billing purposes.

From issues pertaining to this thesis, the directive directly deals with issues surrounding unsolicited communication (SPAM), data related to geo-location, cookies and others.

Article 15 of this directive is particularly important for forensic computing, since it allows for legislative measures that may need to be necessary for successful investigation, data collection and monitoring in cases of investigation of criminal, illegal and other inappropriate activities.

Cybersecurity (sic)[4] Act of 2009 ("Cybersecurity Act of 2009," 2009) proposal in USA that has been introduced in the first week of April 2009 by senators John D. Rockefeller (D-WVA) and Olympia Snowe (R-ME) introduces legislation that would establish new role of 'National Cybersecurity Officer' responsible directly to the White House. This officer would have power to monitor and control Internet traffic to protect against threats to critical information infrastructure (CII). President of the USA can under the proposed Act declare 'cybersecurity emergency' and shut down or limit Internet traffic 'in any critical information network' in the interest of the national security. It is important to note, that the proposed Act does not contain the definition of 'critical information network' or the 'cybersecurity emergency'. The decision is left to the president of the USA, giving him virtually unlimited control over the Internet.

In this regard, it is important to realise that there does not seem to be generally accepted definition of critical information infrastructure (CII), but EU is extensively using definition introduced in Green Paper on European Programme for Critical Infrastructure Protection (Commission of European Communities, 2005). This document defines CII as

[4] Please note spelling of the word – many authors prefer to use two words as in 'cyber security'; however, this particular legislation strictly uses one word and consequently it is expected that this will be used instead of two words in the future.

"ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computer/software, Internet, satellites, etc.)."

Additionally and according to MEMO/09/141 (Commission of European Communities, 2009), OECD defined CII in 2008 as

"those interconnected information systems and networks, the disruption or destruction if which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy."

It is important to note, that European Commission (EC) is not proposing mandatory but only voluntary measures. According to EC,

"ensuring the security and resilience of CII requires cooperation between public and private actors, which is largely based on trust. A non-binding approach will be more effective in steering a dialogue through which interested parties can work out the best way to cooperate and share best practices. During the consultation process prior to the launch of this initiative, Member States' and private sector representatives strongly supported the proposed initiative and confirmed the need and willingness to cooperate at EU level, as long as this remained voluntary".

However, it is also necessary to note that the document does not preclude possibility of using biding/mandatory approach when feasible and useful.

2.5.2 Forensic Computing and the Law

In this context, it is evident that a large number of the issues discussed above have direct relevance for forensic computing and forensic computing investigations. Usefully, Brungs & Jamieson (2005) have conducted a review of the key legal challenges for forensic computing. In the study that they have conducted, they identified 17 pivotal legal issues and problems for forensic

computing and later categorised them to three major classifications "*judicial flexibility, privacy and multi-jurisdictional nature.*"

The issues are briefly described below.

Jurisdictional issue relates to the differences between different legislations. The authors considered only issues arising from different legislations within Australia, however, this will apply even more strongly to international legislation frameworks.

Computer Evidence Presentation Difficulties are closely related to jurisdictional issues. Each jurisdiction can have different requirements for evidence presentation and in some cases evidence acceptable in one state may not be acceptable in the other state. This again will be even more complicated in the international framework.

Requirements to "Fire Up" Original issue arises from best practices guides. For example, in the state of Queensland it is a practice to use the original computer in the court. This creates numerous problems and issues; mainly the fact that once the computer is started it will no longer be in the original state as when it was at the time of ceasing it. This is in direct contrast with several best practice guides available (e.g. National High-Tech Crime Unit & Association of Cheif Police Officers, 2003; U.S. Secret Service, IACP, & DOJ, 2006).

Computer Literacy in the Legal Sector issue is directly arising from the fact that many judges are old and technologically challenged. This creates problems in them understanding digital evidence.

Confidential Record, Business Systems issue relates to the fact that during collection of electronic evidence and/or evidence discovery, privileged rights might be breached.

Telecommunication Act (1979) Covering Data. This issue considers potential implication of the act on data interception. This federal act is supposed to provide privacy protection for data transmission. There is a

question whether this act covers only transmission of the data or also storage of such data.

Criminal Prosecution versus Civil Trial. It is clear that there are differences between requirements for investigation for criminal or civil proceedings. The authors raise question about powers given to private investigators and/or consulting companies in cases where they investigate for example for company that is not prepared to prosecute. While police can obtain warrants in order to recover evidence, these organisations cannot do so and have to rely on different mechanisms to do so.

Privacy Issues and Workplace Surveillance issue has been triggered by introduction of privacy legislations in Australia and is problematic in Europe due to EU Directive on the protection of individuals with regards to the processing of personal data and on the free movement of such data (European Parliament & Council of the European Union, 2002). According to the authors, these provisions have not been adequately tested and as such create primary concern again for private consulting firms.

Interpretation of Telecommunications Act (1997) issue raises concerns about interpretation given in the act to the fact when communication occurred. This is highlighted in a case of e-mails, as it is not clear when to consider e-mail as read or un-read, but this can be extended to question when e-mail is considered to be delivered etc.

Access and Exchange of Information issue again relates to privacy. Authors argue that it is, for example, still unclear when ISP can provide its data to law enforcement and even what information they can gather.

International Cooperation in Practice. From the nature of the computer crime, it is clear that international cooperation is essential. While there is agreement that this cooperation is necessary, there appears to be limited research on how to actually conduct such cooperation. Such research should

include questions of compatibility of different jurisdictions and should influence development of new legislation.

Revision of Mutual Assistance issue relates closely to previous issue. While there are treaties allowing such assistance in place (e.g. Department of Foreign Affairs and Trade, 1997), they are of limited use due to their inflexibility. For example, they do not provide for real-time work.

Contrast of Broadcast versus Communication issue concentrates on differences between communication and broadcasting. For example, in Australia these two modes of information transfer are covered by two different acts – Telecommunication Act (1997) and the Commonwealth Copyright Amendment (Digital Agenda) Act 2000.

Are New Offences Needed? There is a tendency to introduce new offences in relation to electronic and digital communications. The questions are being raised if the newly created offences are enough 'technologically neutral' to avoid recurrent amendments of new laws and codes. It is noted that current Model Criminal Code does not cover piracy.

Launching Actions against Unknown Persons in a Civil Trial. This issue again highlights the difficulty that private sector faces when obtaining evidence. For example, to receive subpoena to identify offender from communication company in civil litigation, civil case must first be launched; however, it is impossible to launch civil action against unknown person.

Technical Issues – Testing of Tools and Techniques issue deals with the fact that forensic experts use different tools. It highlights the need for third party independent validation of these tools to guarantee repeatability and verification of techniques used by various experts. This also closely relates to best practices issues raised earlier.

Qualifications - Expert Witness Skills and Techniques. The authors argue here for definition of skills and qualifications for forensic computing practitioners.

It should be noted that the study on which Brungs & Jamieson (2005) build their conclusion was limited to Australia and included only 11 participants.

2.5.3 Some Other Dude Did It (SODDI)

At this point it is appropriate to discuss some of the new defensive tactics used by defence lawyers in cases involving digital evidence.

The first one involves a tactic widely used and often referred to as 'some other dude did it' or SODDI. In the area of digital evidence it is also referred to as the 'Trojan horse type defence' (Brenner & Carrier, 2004).

Trojan horse is a type of malware, often incorrectly called a virus. However, in comparison to a virus, this type of malware is not self-replicating. It often presents itself as a piece of software doing something else that may be desirable to users (e.g. data cleansing) and while it may or may not actually do this, it also contains the malware. The name comes from Greek mythology about the large wooden horse containing enemy warriors inadvertently brought into Troy. Often, the purpose of Trojan horse is to give the attacker or hacker remote access to targeted computer. It is exactly this fact that is used by lawyers as the basis for the SODDI defence.

Haagman & Ghavalas (2005a, 2005b) provide a review of several cases where the SODDI was successfully used (for example Regina v Aaron Caffrey, Southwark Crown Court, 17 October 2003) and issues that this type of defence creates for forensic computing. The first part of their work provides a good general overview of Trojan horses and how they can be constructed including two scenarios of simple and more complex Trojans using packers. They suggest the necessity to include not only static information gathered from the computer, but also the volatile and network information in the process of an investigation. In the second part, they provide examples of how to conduct analysis and they conclude that

> *"when the techniques that have been described in this article are combined with traditional host based computer forensics, it is clear that*

a forensic analyst is in a much stronger position to be able to prove or disprove a backdoor claim."(Haagman & Ghavalas, 2005b)

Carney and Rogers (2004) claim that "*as yet, there is no reliable way to counter the Trojan defense*" and propose statistical methods for event reconstruction to prove or disprove the SODDI claim. This is a useful attempt to develop a standardised method for event reconstruction with measurable accuracy and significance.

While this type of possible defence creates problems for forensic analysts hired by prosecutors, the use of Trojan horses have recently acquired another, much more worrying dimension. Recently, the Council of the European Union has recommended that Member States should undertake clandestine remote searches of computers of suspects, if provided for under national law and there have been calls for legalisation of spyware, key-loggers and Trojan horses in a recent Australian government commissioned report (Kim-Kwang, 2009). While it is clear that use of such tools could have significant benefit in the investigation of on-line crimes (for example in cases as appalling as child sexual offences), it also creates significant privacy and other legal issues that need to be addressed if an appropriate balance of rights is to be maintained.

Alongside the SODDI type of defence, it is also useful to briefly mention some other more unusual related legal defences that have been used for particular on-line behaviours, e.g. case where a teenage hacker obtained a 'not guilty' verdict based on a defence that such behaviour was 'computer addiction' ("Bedworth Case - UK," 1993; Kelman, 1999). A related issue that has sometimes been considered relates to the 'last mile' problem that a user is not sufficiently computer literate to have been able to undertaken the on-line behaviours of which they have been accused (Hannan & Turner, 2004).

2.6 Organisational Challenges and Issues

"It appears that far less security is applied to data held in computer systems than is the case for data held in manual systems. Office

workers are familiar with the security requirements of a filing cabinet but not necessarily those of a information system" (Backhouse & Dhillon, 1999).

With developments in electronic commerce, organisations have been quick to recognise the commercial opportunities provided by the Internet. However, most have also become aware of the risks posed by criminal, illegal or inappropriate on-line behaviours by their employees, customers or criminals. In particular, organisations remain concerned about fraud, defamation and loss of reputation, financial loss and the loss of a competitive edge.

In response to the above mentioned issues, organisations have developed policies and procedures to safeguard themselves. However, it can be seen that a lack of understanding of the nature of digital information and users on-line behaviours often means these approaches compound the very problems that they are trying to solve (Broucek & Turner, 2003a).

Additionally, regardless of the effectiveness of organisational approaches, there remains a strong tendency to 'pull the plug' when problems are detected rather than to engage in a systematic investigation, collection and analysis of digital evidence of the on-line behaviours that have occurred (Leyden, 2000; Maher, 2001; Microsoft, 2000; Microsoft UK website Hacked - VIGILANTe Statement," 2001; Mitnick, 2000; Rohde, 2000).

2.6.1 Organisations, Digital Data and End Users

From the perspective of allowing ongoing security breaches for evidence acquisition, it is clear that the 'Rome Labs' case (Christy, 1998), the Mitnick case (Shimomura, 1995), the development and use of 'Honey pots' (Even, 2000) and the tracking of computer espionage (Clifford Stoll, 1988; Cliff Stoll, 1989) provide strong arguments against 'pulling the plug'. These cases illustrate the advantages for forensic investigations of tracking and tracing hackers during ongoing security breaches. On the flipside of this, the well published Microsoft case (B. Bace, 2000; Leyden, 2000; Maher, 2001; 2000;

Mitnick, 2000; Poulsen, 2000; Rohde, 2000; Sliwa, 2000; Verton, 2000; Weiss & Rosencrance, 2000) highlights how sensitive this issue can be, particularly for information and communication based industries. Here business reputation as well as specific commercial data are at risk.

With the increasing incidence of computer misuse and e-crime, public and private sector organisations have increasingly sought ways to respond. These responses have included increased e-security precautions, computer usage policies, monitoring and education as well as in some instances the establishment and deployment of forensic computing investigation teams. Whilst these responses are sensible and understandable, in some cases their implementation has had unforeseen results that have actually impaired the overall security of the organisations concerned. Partly, this results from draconian measures imposed on users of the systems and partly from a general lack of awareness amongst most users of the implications for e-security of their on-line usage behaviours.

A good example of this relates to how some organisations approach the management of relatively insecure Internet applications such as e-mail and WWW browsers. With e-mail for example, awareness of these security weaknesses has resulted in many organisations restricting access to organisational e-mail systems. From the users perspective, this has led to the perception of internal e-mail systems as being 'unfriendly' due to their inaccessibility outside the organisational 'firewall' and/or because organisational policies prohibit their utilisation for private communications. However, as a result of the increasingly important social dimension to e-mail usage most employees solve this 'problem' of limited access to e-mail by subscribing to one of the numerous free web-mail services e.g. hotmail.com, yahoo.com, excite.com, gmail.com etc. This user response in-turn introduces further risks for organisational IS security management, particularly as many employees adopt the 'single password for everything' approach. As a consequence, the same password may be used on organisational e-mail systems as well as on private web-mail accounts which in-turn dramatically increases

the possibility of password sniffing/spoofing type security breaches. These free web-mail services also appear susceptible to a higher incidence of direct or double-click attachment based viruses that can easily migrate to the organisational information systems as a result of employee on-line behaviours.

More significantly, most of these free web-mail systems also allow the checking of POP3 e-mail accounts. Employees using these services are rarely aware that in doing so, they may be allowing unauthorised access to organisational information. Similarly, WWW browsers exhibit many security weaknesses that combine with users on-line behaviours to compound system security management problems. These include the use of cookies; web browser history and cache files being kept on local drives; active pages - using Java applets, Java scripts ActiveX technologies and executable elements in web pages all of which create potential risks for the spread of malware (Broucek & Turner, 2002b).

It should be noted that it is these very insecurities in email and browsers that are most often exploited to create the invaluable resources for the basis of e-forensic investigations, particularly in organisational environment, without need for law enforcement involvement. Access to such a data is usually covered by employee agreements regarding information and communication technology use.

Additionally, access to the Internet through web browsers also creates further privacy issues for users and for system management. For example, many organisations use proxy/cache for speeding up, controlling and monitoring access to Internet by using proxy authentication. Proxy authentication and monitoring can create perceptions amongst users of a modern form of 'Panopticon' (Dishaw, 2002). In particular, this perception can be created if such monitoring and/or authentication are introduced without proper policies and if the purpose of their introduction is not explained to users. Proxy authentication is generally used only for statistical purposes; however it can create a 'big brother' type of surveillance fear amongst the users that can

influence their behaviours in ways that impair overall system security. These examples highlight the need to balance requirements for improved security with those of the right to privacy of employees in a manner that does not compromise the potential for future forensic investigation of criminal, illegal or inappropriate on-line behaviours.

Clearly, a major element in any organisational IS security management approach must be to provide detailed explanations and demonstrations to users on how their on-line behaviours can potentially harm the security of the organisation. If organisations feel the need to have the option of monitoring on-line behaviours or conducting forensic investigations then the staff should be informed of the procedures and the results of any investigations or monitoring. Creating a 'big brother surveillance' perception amongst employees may well be counter-productive in terms of IS security and/or wider organisational goals (Dishaw, 2002).

2.6.2 Forensic Computing and Organisational Responses

From a forensic computing perspective there are also implications of the organisational responses to the incidence of criminal, illegal or inappropriate on-line behaviours when they are detected. This is particularly the case in relation to an organisation's ability to accurately handle digital evidence. As an Australian case discussed by Ajoy Gosh (University of Technology Sydney) and cited in the AusCERT 2004 computer crime survey (Australian Computer Emergency Response Team, 2004, p. 9) illustrates, organisations must examine evidence correctly or face the consequences – the case in question concerned "*evidence of transactions made using a junior clerk's 'userid' that were fraudulent*". The clerk was subsequently dismissed and asked to repay the funds or face prosecution. Both the company and clerk (through the Union) organised for the conduct of forensic examinations of the digital evidence by forensic experts. Subsequently it was revealed by the expert engaged by the clerk's solicitor that "*the suspect transactions were in fact made by a company director pretending to be the clerk*". Significantly, it was also revealed that "*the*

company had requested its forensic consultant to make certain omissions in his report". The end result was that the clerk received a substantial termination payment and agreed to sign a deed of confidentiality, the dishonest company director resigned and paid back the funds and the alleged fraud was never reported to the Police. This case highlights a number of issues that highlight the interrelatedness of organisational, technical and legal approaches:

- Organisational responses, particularly where they are settled 'out of court' are analogous to the technical response to an incident of 'pulling the plug' in that they inhibit the development of understanding on how best to collect, analyse and present digital evidence. This in-turn is inhibiting the development of case law interpretations on acceptable practices, procedures and approaches to dealing with the admissibility and evidentiary weight of digital evidence;
- The case also reveals the importance of examining links between digital evidence and other types of evidence. This in-turn highlights the problem of 'the last mile' (Hannan & Turner, 2004) and the significance of conventional investigative techniques and other types of potentially corroborative evidence.

More broadly, as organisations seek to respond to these challenges, they find themselves in a curious position in relation to law enforcement agencies (who under new legislations are increasingly being empowered to respond). The lack of delineation over responsibility for chain of evidence and chain of custody in relation to digital evidence creates uncertainty and further compounds the development of best practices in terms of technical and legal responses to incidents. Finally, there is also the inter-relationship between research and development into computer misuse and e-crime and organisational demands for e-security.

Anecdotal evidence collected by the author of this thesis suggests that compliance with e-security requirements placed on staff in law enforcement agencies at state, national and international levels is inhibiting the ability of

these agencies to keep pace with the development of malware and new types of illegal or inappropriate on-line behaviours, e.g. some researchers in the field of child pornography have been inhibited from visiting/monitoring certain websites/chat-rooms because of organisational e-security approaches.

While clear safeguards are required, it is important to note that e-criminals do not face any type of restriction on engaging in or developing new on-line behaviours. Indeed, the ingenuity of many types of computer misuse and digital crime display the willingness on the part of perpetrators to use any and all resources at their disposal, to not delineate between domains and to move between digital and physical environments and artefacts on the basis of 'whatever works'.

Another limiting factor is lack of methodologies for documentation and reporting of information technology incidents. Sandra Frings (2006) notes that there are much higher number of IT incidents than it is reported. According to Frings (2006) the two major reasons for not reporting are:

- Non-disclosure due to fear of damaging image;
- IT security incidents not recognised as harmful and even if they are, there is a lack of procedures to deal with them.

Frings continues by suggesting fundamental attributes for IT incident documentation. This should be based on existing standards and practices (for example ISO17799:2005 , ISO/IEC27001:2005, ACPO Good Practice for Computer Based Evidence), but most importantly it has to be:

- Clear and comprehensible;
- Meaningful and reasonable;
- Complete; and
- Structured.

Frings concludes by suggesting that method of structured documentation needs to be added to CTOSE software prototype.

2.7 Emerging Trends

> *"A (isolated) computer is quite never really disconnected from the outside" (Eric Filiol, Black Hat USA 2008)*

The number of publications relevant to this research has significantly increased since 2001 when this research started. As a result, it is acknowledged that the literature review identifies only the key trends and directions across the three domains (technical, legal, organisational) with the aim of highlighting potential intersections that are then explored through the case studies.

2.7.1 Antivirus Research

Josse's (2006) paper makes a useful contribution in relation to the criteria that can be used to assess the effectiveness of anti-virus products. A protection profile for assisting software manufacturers to design anti-virus products in accordance with a Common Criteria standard is advocated and a number of tests that can be carried out to validate the security requirements presented. Josse suggests that use of a protection profile and the specification of tests is a valuable basis for measuring the effectiveness of anti-virus products.

Filiol (2006a) presents a new model of malware detection pattern based on Boolean functions. This paper also describes a combinatorial, probabilistic malware pattern scanning scheme that limits black-box analysis and can only be bypassed where there is collusion between a number of malware copycats.

In another paper, Filiol and Josse (2007) present a statistical model of malware detection revealing how this points to the possibility for the development of undetectable malware. Building on research by Chess and White (2000) they demonstrate how existing detection techniques can be statistically modelled and precise definition of false-positive and non-detection presented. Moreover, they show how statistical model may be simulated in order to deceive antiviral detection. They conclude their paper by presenting a statistical variant of Cohen's (1986) undecidability results of virus detection.

Some of these ideas are further developed by Filiol (2007). In this paper Filiol illustrates a new class of codes (potentially malicious) called 'k-ary codes'. Instead of containing the whole instructions composing the program's action, these type of codes are composed of k distinct parts (each containing a subset of the instructions) which constitute a partition of the entire code. As a result, each part cannot be detected by anti-malware programs from conventional program code. Filiol proceeds to present a formalisation of these codes using Boolean functions and presents detailed taxonomy. The paper concludes that besides a huge number of beneficial applications using k-ary codes (e.g. protection against software piracy), these codes represent a potentially huge risk in terms of the generation of new malware. According to Filiol 's experiments, existing antivirus technologies are totally inefficient at detecting those codes since the detection has to face combinatorial problems that cannot be solved in an amount of time that is compatible with most commercially available antivirus software.

Bayer, Moser, Kruegel & Kirda's (2006) paper presents TTAnalyze, a tool for dynamically analysing the behaviour of Windows executables. This tool runs binaries in an unmodified Windows environment and they argue that this leads to excellent emulation accuracy and makes the TTAnalyze tool ideal for quickly getting an understanding of the behaviour of an unknown malware.

Avlonitis, Magkos, Stefanidakis, & Chrissikopoulos (2007) present a new spatial stochastic model of worm propagation by incorporating non-uniformities within interacting subnets. The authors argue that efficient monitoring strategies can be deployed based on the results of random scan strategies and local preference scan worms.

Ondi and Ford (2007) in their paper on metrics for worm and anti-worm measures argue that there exist no meaningful metrics by which one can quantitatively compare the effectiveness of different protection paradigms. They present several possible metrics for measuring worm spread and countermeasure effectiveness and highlight that the 'correct' metric for

comparative purposes will vary depending on the goal of the defender. They conclude by discussing what changes induced by worm design or countermeasures are actually meaningful in the real world.

Aycock, deGraaf & Jacobson's (2006) paper presents a new method of anti-disassembly based on cryptographic hash functions which is portable, hard to analyse, and can be used to target particular computers or users. They suggest that the obscured code is not available in any analysable form, even an encrypted form, until it successfully runs and that they have been able to empirically validate their results. The authors then proceed to examine possible countermeasures for this basic anti-disassembly scheme, as well as variants scaled to use massive computational power.

In Vinoo and Nitin's (2007) paper the focus is also on practical measures but here in relation to counter-measures against bots on organisational internal networks. The authors argue that organisations should not rely only on their security vendor's protection against this type of malware but rather should develop their own intelligence gathering methods to improve protection. More specifically, the authors propose setting up an IRC honeypot on internal networks to function as an early warning system against bot-like activities. They argue that such a system can be set up with minimal effort and investment but can provide significant assistance in the fight against these types of malware.

2.7.2 Computer Security

Kayayurt & Tuglular's (2006) paper explores the use of end-to-end security protocols, specifically Transport Layer Security Protocol (TLS), in mobile devices for ensuring maintainability and extensibility. The authors then examine cryptographic operations via the use of the Bouncy Castle Cryptography Package (see http://www.bouncycastle.org/documentation). Their implementation has been tested with a variety of cases and they argue that the object oriented architecture of this proposed end-to-end security

protocol implementation makes the replacement of this library with another cryptography package easier.

Related to concerns with internal organisational security problems is Josse's (2007) paper on rootkit detection which presents a secure engine specifically designed for the security analyst to analyse rootkits and related programs that interact deeply with operating systems, including AV, FW and HIPS. This paper presents 'state-of-the-art' algorithms for rootkit detection and reviews forensic techniques and advanced heuristics. Interestingly, the paper uses a human analysis framework to conduct comparative analysis of security aspects of security products like AV, FW, HIPS and deals with the robustness of their driver stack and the quality of their implementation. The paper also proposes a reliable system for automatically gaining information about a rootkit and its interaction with the OS executive (stealth native API hooking and kernel objects integrity checking).

One of the latest developments in computer security is related to the notion of The Biologically-Inspired Tactical Security Infrastructure (Carvalho, Ford, Allen, & Marin, 2008). As mobile ad-hoc networks (MANETs) become increasingly important (particularly in the areas of cyber warfare), it is even more important to protect these networks against security breaches and cyber attacks. These systems are highly collaborative and in mode of constant change in traffic, resources and topology. This research proposes novel approach based on concepts of artificial immune systems and danger theory. This is starting, cutting edge research and it remains to be seen how successful it will become.

2.7.3 Cyber Crime

Gordon & Ford (2006) adopt a high level conceptual approach in their analysis of on-going discussions and definitions of computer crime that they view as creating confusion amongst academics, industry experts and governments. Following a re-definition of terms, the authors present two case studies to illustrate the role of crime-ware and offer some observations on the role of cognition in the process of cyber crime.

Preuß, Furnel, & Papadaki (2007) explore the potential of criminal profiling for combating hacking based on the results of German case studies. The paper presents the commonalities and differences in motive and modus operandi (MO) identified in the twelve case studies provided by the Bundeskriminalamt[5]. The authors conclude that a basic principle that can be identified is that despite differing motivations hackers tend to take the path of least resistance in making their attacks.

Coles-Kemp and Overill (2007) argue for the need for a specialised facilitation role in information security risk assessment. The authors suggest that without this role the possibility of generating outputs that are meaningful for businesses to act upon are much reduced. Their point of view is supported by reference to field observations of certification audits of a number of organisations combined with the standard models of BSI/ISO/IEC and FRAAP.

Gattiker (2007) examines the issues of information assurance and education in the light of the Bologna Declaration (see http://www.ond.vlaanderen.be/hogeronderwijs/bologna/). The paper focuses on European undergraduate and graduate education efforts in the area of computer security. Following an analysis of the issues the paper summarizes key findings and practical implications for European information assurance processes into the future.

Educational issues are also a concern in Li and Helenius's (2007) paper on the use of anti-phishing toolbars. Based on a usability evaluation, the authors highlight issues and propose mechanisms for improvement particularly in relation to the client side of the available tools.

Jorns, Jung and Quirchmayr (2007) argue that without the implementation of proper privacy protection contextual information processed by 3rd party application providers may present privacy risks to end users. To address this problem the authors present a novel service architecture which fosters the

[5] German Federal Criminal Police Office

development of innovative applications but contains an underlying privacy enhancing mechanism that is based on the notion of pseudonyms. This service architecture is demonstrated through a transportation ticket application that supports location-tracking functionality.

2.8 Summary Reflection on the Chapter

In each area examined in the literature review, it is clear that digital evidence and its acquisition, analysis and presentation post challenges for technologists, law makers, law enforcement and business leaders. The responses in each of these areas are complex, constantly evolving and significantly only partial. Each stakeholder group involved is trying to generate coherent responses in their respective areas. Significantly, however, the inter-relationships between areas and responses generated have rarely been investigated and consequently are poorly understood. A major concern that underpins the approach outlined in the next chapter is the need to understand how these inter-relationships impact on the overall effectiveness of responses in each area.

3 Research Methodology

"Research is to see what everybody else has seen and to think what nobody else has thought" (Albert Szent-Gyorgyi, 1937)

3.1 Introduction

This chapter presents the research method used to conduct this research. The methodological framework underpinning this research adopts a subjective ontology and employs an interpretative epistemology. The research strategy involves the examination of three cases on technical, legal and organisational challenges of digital evidence respectively. Each case is analysed independently to find key issues of the area. The interpretation and discussion adopts a forensic computing perspective to interpret and discuss the inter-relationships across these areas and to explore the implications for digital evidence and the underlying problematic on-line behaviours. Case A examines the validity of quantitative data collected by running a network intrusion detection system (NIDS) SNORT on University network. Case B examines an Australian Federal Court case illustrating legal arguments applied to digital evidence, its discovery and presentation. Case C examines the Cyber Tools On-line Search for Evidence (CTOSE) project highlighting the difficulties of developing and implementing organisational level processes for digital evidence handling.

The first part of this chapter provides detail on the selected research philosophy. The second part details the research strategy used for this research. The third part of this chapter provides the research design used for each case. The fourth part provides detail on the approach to data analysis adopted for each case. The last section provides detail on the selected approach to interpretation and discussion.

3.2 Research Philosophy

This research is of an exploratory nature, seeking to examine key technical, legal and organisational challenges in digital evidence in each area through three case studies independently and then employs a forensic computing perspective to explore the key inter-relationships between the areas. It also seeks to discover what implications these inter-relationships have for the future development of the responses to the challenges of digital evidence and the underlying problematic on-line behaviours.

3.2.1 Ontology

Ontology in philosophy is the study of the nature of being, existence or reality in general. More generally, ontology is a theory or study of existence and refers to the nature of the world around us. Ontology deals with questions concerning what entities exist or can be said to exist, in other words, if the world around us is considered to be objective or subjective (Burrell & Morgan, 1985; Orlikowski & Baroudi, 1991).

According to Neuman (2000) exploratory descriptive research is useful to

> *"clarify a sequence of steps or stages"*, to *"report on the background or context of the situation"*, and to *"become familiar with the basic facts, settings and concerns."*

A subjective ontological view can be described as one, which emphasises the subjective reasoning through which humans construct their own reality (Orlikowski & Baroudi, 1991). It implies that the researcher assumes that the social world is produced and reinforced by humans through their action and interactions. In exploring inter-relationships across cases, this research acknowledges the importance of subjective reasoning of technical, legal and organisational experts.

3.2.2 Epistemology

Epistemology describes how the world is perceived by the researcher, and the relationship between the researcher and reality. The nature of the research questions selected for this research indicates the need for subjective interpretation of the data. This includes interpretation of the data generated through statistical methods in the Case A. An interpretative research approach is considered to be the most appropriate to identify and analyse factors within each selected area and to explore the inter-relationships between them through the adoption of a forensic computing perspective.

The aim of this research is to gain a deep understanding of underlying key technical, legal and organisational challenges and to examine the key inter-relationships between these areas.

In conclusion, a methodological framework using subjective ontology with an interpretive epistemology was most appropriate for the exploratory nature of the presented research. The next section provides a description of the research strategy.

3.3 Research Strategy

The research strategy involves the examination of three cases on technical, legal and organisational challenges of digital evidence respectively. Each case is analysed independently and the interpretation and discussion explores the inter-relationships between the cases and their implications for digital evidence and on-line behaviours.

3.4 Research Design

> *"Though this be madness, yet there is method in 't."(William Shakespeare, "Hamlet", Act 2 scene 2)*

Building on the three-case strategy, the research design for this investigation involves three sets of data collection techniques across the three cases.

3.4.1 Technical Data Collection for Case A

The data for this study was collected on a production server operated by one of the schools at the University of Tasmania in August and September 2002. This server was used for providing web services and non-anonymous file transfer protocol (ftp) access for updating school's antivirus software clients. It was running on dedicated hardware unit. The data collection was conducted as a part of day to day operations of the system and as such was considered as normal business operation.

3.4.2 Legal Court Documentation for Case B

This case study is based on transcripts and judgements from Sony Music Entertainment (Australia) Limited v University of Tasmania case heard in the Federal Court of Australia ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003)," 2003; Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 724 (18 July 2003)," 2003; Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003)," 2003; Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 929 (4 September 2003)," 2003). In this case, Sony Music Entertainment was seeking discovery orders in relation to alleged copyright infringement by members of several Australian Universities. In this thesis, proceedings against University of Tasmania in particular are followed. The researcher was also able to consult directly with some of the key IT personnel involved in the case.

3.4.3 Organisational Data from CTOSE Project for Case C

This case study is based on a detailed analysis of data and documentation from the CTOSE project. This data was collected as part of researcher's involvement and collaboration with the CTOSE project.

3.5 Approach to Data Analysis

Building on the research design above, this section describes the approach adopted for the conduct of analysis from each of the three cases.

In each analysis chapter, the actual data analysis is conducted using a range of techniques, including statistical analysis, documentation analysis, and the analysis of observations and interview data. Throughout the analysis of each case, the researcher maintained a forensic computing perspective to ensure sensitivity to potential inter-relationships amongst the three data sets. Each analytical process used in each case is described in the following sections.

3.5.1 Case A - SNORT

The analysis of the case is based on SNORT's own outputs – alerts, log files and traffic collected in 'tcpdump' format ("tcpdump/libpcap," 2002). These files were assessed using expert knowledge of the administrator responsible for the system and with additional help from University wide administrators and experts on networking.

Traffic data collected in 'tcpdump' format were analysed using two common free (under GNU licence) tools – 'tcpdump' ("tcpdump/libpcap," 2002) and Ethereal ("ethereal," 2002) programs in addition to SNORT's own outputs. These tools were used on both UNIX based and Windows 2000 based workstations to eliminate possible bugs. Results received on both platforms were identical; however, small but from forensic computing perspective significant differences were observed between the two tools. In particular, the time resolutions used and the different amounts of detail provided in the outputs.

Finally, the author had an opportunity to analyse and visualise collected traffic using commercial CA eTrust Network Forensics in 2005/2006. Unfortunately, significant bug was discovered in the tool's capability of acquiring and visualising these data and this part of the analysis was dropped from the thesis

due to commercial implications and limited capability of full reporting due to a non-disclosure agreement with CA. However, this fact supports one of the key findings of this research.

3.5.2 Case B - MP3

The analysis involves detailed critical analysis of the court rulings, together with analysis of available transcripts of court proceedings. Some additional insider knowledge and analysis was conducted by talking with UTAS personnel directly involved in initial response, preserving the evidence and testifying during the court hearings.

3.5.3 Case C - CTOSE

The analysis involves a detailed analysis of the CTOSE framework and a review of its achievement and results following completion of the project. As a result of the researcher's close collaboration with the CTOSE project, this analysis is able to examine some of the key issues that inhibited the framework's commercialisation, adoption and use by organisations for whom it was developed. This analysis is conducted in the context of the project having gained wide spread recognition, substantial financial support from EU and its results being considered to be a highly successful solution to the problems it identified.

3.6 Approach to Interpretation and Discussion

Interpretation and discussion of the analyses from the three cases adopts a forensic computing perspective and focuses on the nature of the inter-relationships between the issues identified in each case. From this perspective the discrete approaches adopted in each case limit an appreciation of the complex interplay between technical, legal and organisational factors, an interplay that because of the nature of digital environments continues to have serious implications for each of these areas. More specifically, this interpretation and discussion reveals how and why this continued

fragmentation of discrete approaches is impairing the overall effectiveness of the responses developed. A consequence of this is the lack of integrated and coordinated solutions that would effectively balance requirements for legally admissible digital evidence, effective e-security and data privacy.

3.7 Summary Reflection on the Chapter

This chapter has presented the research methodology used in the conduct of this research. It has outlined the research philosophy, research strategy, and research design used in a three case approach. This chapter has also presented detail on the conduct of the data analysis, interpretation and discussion.

The next three chapters (chapters 4, 5, 6) present analysis from each of the three cases. Chapter 7 adopts a forensic computing perspective to explore their inter-relationships.

4 Data analysis Case A – SNORT[6]

"The bad guys can essentially defeat most forensic computing efforts on standard hardware with ease ONCE the case law starts to get put in place. Anti-forensic tools pose a serious threat to the usability of electronic evidence" (Ford, 2008)

4.1 Introduction

This case provides a case study on the network traffic data collected by SNORT (Roesch, 1999, 2001a, 2001b) network intrusion detection system (NIDS) on a University school World Wide Web server over a two-month period. At this point, it is necessary to stipulate that this case study is based on the data collected by running SNORT as a part of 'normal' business operations, although some adjustments have been made to ensure consistent data. Further, it is not the intention of this study to evaluate the SNORT IDS. No comparisons are being made concerning the relative merits of SNORT against any other free or commercially available IDS systems and all the conclusions made in this study would apply to IDS in general. The case study is analysed and discussed from a forensic computing perspective. This perspective considers the nature of the intrusion detection and network monitoring security provided and evaluates the system in terms of its evidence acquisition ('forensic') capabilities and the legal admissibility of the digital evidence generated. It also discusses privacy implications that the deployment of IDS creates and illustrates them with examples from the collected data. The SNORT system was selected primarily because of its easy availability (i.e. being free, open source software) and its widespread use in Universities, public institutions and many large commercial organisations.

---

[6] Please note some of the material presented in this chapter has been adapted from materials first published in the following peer reviewed publication:

Broucek, V., & Turner, P. (2004). Intrusion Detection: Issues and Challenges in Evidence Acquisition. *International Review of Law, Computers and Technology, 18*(2), 149-164.

Hardware

The server was based on an 'off-the-shelf' Intel Celeron 300 computer with 256MB RAM and 3GB IDE hard drive. The server was connected to 100 Mbit/sec port on a Cisco 2900 series switch that was further connected to the University backbone network. The server was located inside the University's network that contains more than 10,000 registered hosts. This network is protected against unauthorised access from the Internet by Cisco PIX firewalls. During the study, access to the server from the Internet was initially possible only on TCP/IP port 80 (http protocol) and after 30 days access was extended by enabling encrypted access on port 443 (https protocol). The server was not located in the demilitarised zone (DMZ) and as a result the computers connected to the internal University network had full access to the server. Although this was not an ideal situation because of an associated increase in security risks, it is very typical of University schools' WWW servers. Subsequently, this practice has been disallowed at the University of Tasmania and all www services are now hosted on dedicated server within central Information Technology Resources data centre and located in DMZ.

Software

The server was using Sun Solaris 8 operating system. This operating system was completely patched on 31 July 2002 and the case study was conducted during the period 1 August to 30 September 2002. To maintain the integrity of the collected data sets, no further OS and application software patching was done during the period of the study.

In relation to the software set-up used during the study standard security precautions based on AusCERT recommendations (Australian Computer Emergency Response Team, 2001a, 2001b; Smith & Indulska, 2001) were made prior the data collection. Among these, TCP Wrappers (Venema, 1992) were installed and configured to limit access to services run on the server. Non-essential services, for example, telnet and tftp, were completely disabled. The web server was for the first 30 days of the study running Apache 1.3.26 http

daemon ("Apache HTTP Server," 2002) with Microsoft FrontPage 2002 server extensions. The MS FrontPage extensions were used for web authoring, as well as for collecting data from students using built in form tools. Subsequently, the server was extended to support encrypted SSL connections using mod_ssl version 2.8.10 ("mod_ssl," 2002) and openssl version 0.9.6g ("openssl," 2002). The ftp server was using the standard ftp daemon provided in Solaris 8, with TCP Wrappers limiting access to this server from two particular class B sub-networks within the University. Anonymous access to ftp server was not enabled at all. This ftp server provided updates for McAfee antivirus software used in the school. An in-house developed Perl based program contacted McAfee's master site twice daily and checked for the availability of software updates. If the updates were available, it downloaded them and sent an e-mail to the administrator. All IBM-PC hosts in the school (around 150) running various versions of Microsoft Windows were set up to contact this server every morning between the hours of 06:00 and 08:00, to check for the availability of update files and download them. The only additional access to the server was through ssh. The server was running ssh daemon version 3.2 ("ssh," 2002) and access to ssh daemon was again limited using TCP Wrappers to certain networks only.

Three 'name based' (see Apache documentation at http://httpd.apache.org/doc/) virtual web servers were running on the server. Two of these servers were accessible from the Internet on port 80 (http protocol). After thirty days of the study one of these two Internet-connected virtual servers was also made accessible on port 443 using Secure Socket Layer (SSL) for encryption. The third virtual server used '.htaccess' method to limit access from within the University networks only. However, being a 'name based' server and sharing same TCP/IP addresses with other two virtual servers, it was in some sense 'visible' to the Internet.

Although SNORT (Roesch, 1999, 2001a, 2001b) is typically used as a network intrusion detection system (NIDS), it has been set up and installed directly on the web-server in this school. There were several reasons for this, including

that the primary focus was in monitoring only this particular server. After several months of testing with two different versions of SNORT on both UNIX and MS Windows platforms, version 1.8.7 was installed on 31 July 2002 on this server and started with a default, up-to-date rule set on 1 August 2002. The only modifications made to SNORT's default configuration files were to define 'home' and 'external' networks, and to instruct SNORT to collect all traffic in 'tcpdump' format. Due to the fact that the University's environment can be considered 'hostile', the 'external' network was set up as 'any network' with the exception of two 'trusted' hosts maintained and used solely by the author of this research.

4.2 SNORT Data Collection Experience

From the very first day of running the system, it was clear that Intrusion Detection Systems present many problems as reliable sources of intrusion alarms. To ensure they operate at their optimal levels requires highly trained network professionals and considerable efforts in fine-tuning the system. In the first several hours of being on-line, SNORT produced large amount of alarms caused by regular network traffic. The default rule set used at the start of the experiment is set to trigger low level alarms on many types of such traffic. The source hosts for these alarms were from all around the University network but mainly from the central Information Technology Services (ITS) department. This department provides a range of services that would regularly give reasons for alarms to be triggered including DNS, BOOTP/DHCP and SNMP network management.

To eliminate these false alarms, it was necessary to adjust the system configuration files as well as the rule sets by making decisions on whether the hosts identified as the sources of these alarms should be treated as 'trusted' hosts or not. As a result of this fine-tuning, ITS hosts were treated as 'trusted' and this immediately reduced the number of false positive alarms. This is not, however, an ideal situation when fine-tuning IDS. Although the majority of these hosts were dedicated hosts managed by well-trained administrators, some

of these administrators may have a lack of understanding of several security issues related to services run on their hosts. This in-turn may lead to undetected security breaches.

One finding came from an analysis of regular alerts triggered by one of the central hosts broadcasting 'rusers' requests. Because 'r' commands are considered to be one of the least secure commands in the UNIX world, alarms concerning these activities were raised by both TCP Wrappers and SNORT. It has been found that these requests were generated by the CiscoWorks suite used by the University for managing its Cisco based network. This suite regularly tries to do 'rusers' queries on every host known to it. It is surprising that Cisco is still using something that has been considered to be insecure and a source of information leaking.

Further sources of alerts were triggered by a variety of other hosts around the University. One particular alarm was triggered by hosts trying connection on UDP port 161 (SNMP – Simple Network Management Protocol) using a default 'public' string. This was of particular interest due to, at that point recent, recognition of the vulnerability in SNMP protocol implementations. Investigation of these alarms discovered that they were triggered by HP JetAdmin and HP WebAdmin suites installed on these hosts. These suites can be set up to look for HP printers in regular intervals and then to check each printer in their databases regularly. Again, a decision had to be made as to whether these hosts should be 'trusted' or not. It was found that it is impossible to trust these hosts because in some instances they were not dedicated servers, for example, an MS Window NT 4 workstation used by a postgraduate student and an MS Windows 2000 Server that was not being maintained by an IT professional. It was later confirmed that this particular W2K server was running a default installation that had not been patched for several months and was as a result vulnerable to several security issues current at that time.

Day two brought more false positive alarms as well as alerts indicating attempted attacks exploring the web server's vulnerabilities from the Internet.

These attempts mainly focused on known vulnerabilities in Microsoft IIS server. These attempts were futile, because of the Apache software running on the server. In one particular case, a host based in Denmark continued to attempt gaining unauthorised access to the web server three times a day over several days.

The first alarm of the second day was triggered by NOP86 rule on a connection from a host with a non-functioning reverse DNS lookup. Furthermore, this alarm was triggered on a connection initiated by the server that was running the IDS. Further investigation revealed that it was an ftp connection to Network Associates site initiated from the server for McAfee antivirus software updates - these updates having been found and downloaded by the server. The question as to why this activity triggered an alarm is surprisingly simple. One of the virus signatures in the zipped file exactly matches the NOP86 attack signature. This gave rise to a dilemma - was it possible to declare the McAfee server to be a 'trusted' host? The decision was made to do so, however, the alarm was triggered again in the afternoon during a second update triggered by a different host. Unfortunately, Network Associates provides (quite understandably) updates from a server farm where TCP/IP numbers can be different every time. The question remains why McAfee does not have a properly set up reverse DNS lookup. At the time of running the experiment, Network Associate's master site for McAfee antivirus software ftp.nai.com resolved to 161.69.201.237 and 161.69.201.238. However, reverse lookup on both addresses did not resolve back.

Similar problems arising from incorrect reverse DNS lookup were observed later in relation to one visiting web crawler/spider. In this case, the research section of one of the Blue Chip IT companies running the crawler was contacted and the issue was resolved very quickly. The crawler was based behind the company's firewall and was being assigned a dynamic TCP/IP address without a proper DNS entry.

During the second and subsequent days more false positive alerts were triggered. Many of them remained unexplained – for example why Netware 5.1 servers quite regularly trigger 'Possible evasive RST' alerts; and why filling in a MS FrontPage form on the web server and submitting it triggers several MS FrontPage vulnerability alerts. One possible explanation of this last point may be that SNORT's 'default' rule set is not detailed enough to recognise this form of FP extensions usage as legitimate and for reasons stated before it was impossible to consider departmental computers in the labs as trusted.

For the rest of the month data were collected and no further adjustments were made to the rule sets or SNORT's configuration to ensure comparable data was collected under the same rule set and configuration. It was also decided not to update the rule sets or configuration during the remainder of the experiment for any newly discovered security threats. Such a decision would be totally unacceptable in a commercial environment; however, in the context of this study it was acceptable because the departmental web server does not hold any commercially valuable data and mechanisms were in place to ensure that data and server could be restored quickly without any losses.

One bug in SNORT version 1.8.7 was identified during this period. Its analysis and implications are discussed further in this thesis.

At the beginning of the second month, the server was extended to provide for the secure socket layer (SSL) capability, providing the duplicate information from one of the virtual servers on port 443 (https) in addition to standard port 80 (http). The reason for this was to prove that signature based intrusion detection systems would not be able to detect any attacks conducted over SSL. An internal host was used to try to exploit several known security issues. As expected and quite understandably, none of the attacks were detected by SNORT. However, it was possible to observe them in the web server's log files.

Monitoring continued in the same fashion, again without any updates or further tuning of the system, and further data were collected. Several hosts on the

Internet discovered that the server was running also on port 443 and several attempts on that port were recorded in the log files of the server. However, as expected, none of these attempts were detected by SNORT. Indeed, again as expected, even detailed analysis of traffic data using ethereal and tcpdump did not provide any more information than that there was encrypted traffic flowing between two hosts.

4.3 Analysis of Data Collected for Case A

Data for this experiment were collected from 1 August 2002 till 30 September 2002. Overall, there were 2669 alerts triggered during the period, with first trigger on 1 August 2002 at 00:33:43 EST (GMT+10) and last trigger on 30 September 2002 at 18:30:19 EST. These triggers were coming from 301 different sources and had 41 different signatures.

The first step was to eliminate the false positives. This process was gradual through the whole period of the experiment and each trigger was investigated using available tools and contacts. 1212 triggers were identified as false positives and 1457 triggers remained.

Out of these, 540 (more than 33%) were found to come from domains within Denmark. These findings are summarised in Figure 6.

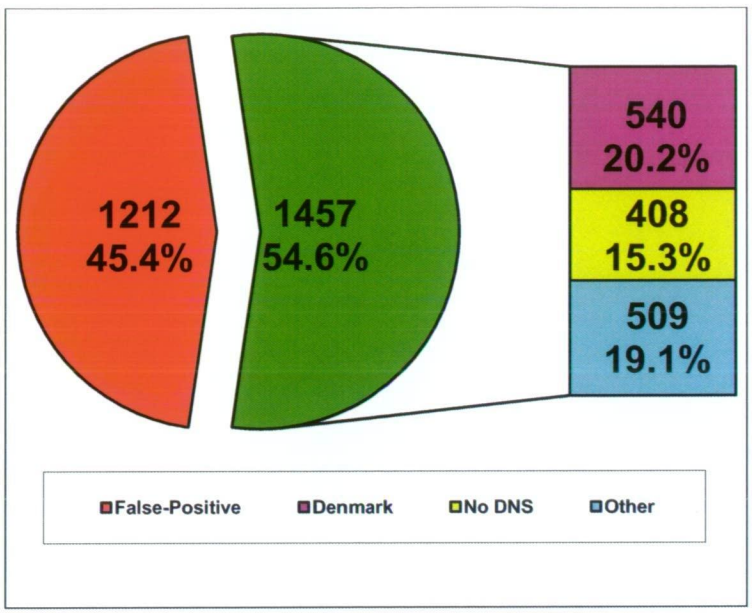


Figure 6: False Positive versus Positive Alerts

Most of the hosts triggering the alerts were mainly coming from Denmark and as their FQDN suggested, these were using ADSL (asymmetric digital subscriber line) connections. There is a well-founded suspicion that many of these attacks were launched automatically from infected machines and the owners/users of these computers were not aware of what was happening on their hosts. A further 408 alarms were from hosts with TCP/IP addresses without domain name service (DNS) entries. These hosts' TCP/IP addresses did not resolve to host names, hence it can be presumed that these hosts were not properly registered with their Internet Services Provider (ISP), or ISP did not provide correctly DNS services. Another possible conclusion is that these triggers were in fact coming from properly registered hosts but using anti-forensics tools and/or other techniques to obfuscate their real identity.

One particular form of attack was most prevalent. It was the exploitation of the Microsoft IIS server via the 'cmd.exe' weakness. Of the total, 592 (22.18%) alerts were of this form of attack. Again, most of these came from hosts based in Denmark. Other forms of attacks that were noted included 83 (3.11%) attempts using 'WEB-FRONTPAGE author.exe' access, 60 (2.25%) attempts using 'WEB-IIS ISAPI .ida' and 46 (1.72%) using 'WEB-IIS CodeRed v2

root.exe' accesses[7]. These statistics clearly illustrate that the majority of attempted attacks tried to exploit known weaknesses of the Microsoft IIS server. This is in spite of the fact that the server being used was running Apache web server software that would be very easy to query before trying to make an attack. Those attackers trying to exploit these weaknesses consequently only succeeded in leaving data about themselves. This leads to the preliminary conclusion that many of these attacks were either initiated by so called 'script kiddies' or launched automatically by infected computers.

4.3.1 Example of Alarm Analysis

This part provides an analysis of one particular alarm that revealed a bug in SNORT version 1.8.7. The same method was used to analyse all other interesting alerts during the course of the trial. The real TCP/IP addresses have been replaced with addresses in form of 'XXX.XXX.XXX.XXX' where they were in 'dotted' form and in form of 'XX XX XX XX' where they were in hexadecimal form. MAC addresses were left intact. It is believed it would be nearly impossible to identify involved hosts from their MAC addresses.

Figure 7 shows the alarm that was raised on 17 August 2002 at 05:15:22.029533. This alert was most probably triggered by a host on the Internet using 'decoy' techniques during scanning for vulnerabilities. However, interestingly SNORT claims that there was communication from port zero to port zero in the original datagram dump part. This is clearly erroneous. To find out what was really happening, tcpdump and ethereal were used to view the actually captured packet. Ethereal's GUI interface unfortunately does not provide for easy copying and pasting of output to documents, hence its less user-friendly 'command line based' brother called tethereal was used for dumps presented in this study.

---

[7] Readers are encouraged to visit computer security related sites to find out more about these attacks. Some examples of good sites to visit are http://www.snort.org/, http://www.whitehats.com/, http://www.auscert.org.au/, http://www.sans.org/ and many more.

```
[**] [1:485:2] ICMP Destination Unreachable (Communication Administratively
Prohibited) [**]
[Classification: Misc activity] [Priority: 3]
08/17-05:15:22.029533 XXX.XXX.XXX.XXX -> YYY.YYY.YYY.YYY
ICMP TTL:242 TOS:0x0 ID:54572 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: ADMINISTRATIVELY PROHIBITED,
PACKET FILTERED_
** ORIGINAL DATAGRAM DUMP:
YYY.YYY.YYY.YYY:0 -> ZZZ.ZZZ.ZZZ.ZZZ:0
UDP TTL:126 TOS:0x0 ID:7936 IpLen:20 DgmLen:71
Len: 51
** END OF DUMP
```

Figure 7: Alarm Raised by SNORT

First, the packets were printed in hexadecimal/ascii format. This is the simplest possible format to print, however its analysis requires significant knowledge of packet structure, theory of TCP/IP networking and all the protocols involved. Both tools provide simple decoding of the packet together with the hex/ascii dump. Also note time resolution differences between Figure 8 to Figure 9.

```
Frame 226 2002-08-17 05:15:22.0295 XXX.XXX.XXX.XXX -> YYY.YYY.YYY.YYY ICMP
Destination unreachable
0000  00 30 c1 0a 82 6b 00 04 9b 2f e3 fc 08 00 45 00   .0...k.../....E.
0010  00 38 d5 2c 00 00 f2 01 ca 48 XX XX XX XX YY YY   .8.,.....H.n....
0020  YY YY 03 0d 55 6e 00 00 00 00 45 00 00 47 1f 00   #...Un....E..G..
0030  00 00 7e 11 e1 7f 83 d9 23 06 ZZ ZZ ZZ ZZ 00 89   ..~.....#..=....
0040  00 35 00 33 a6 93 93 a6 4b 71                     .5.3....Kq
```

Figure 8: Hexadecimal output using tethereal

```
05:15:22.029533 0:4:9b:2f:e3:fc 0:30:c1:a:82:6b 0800 74: XXX.XXX.XXX.XXX >
YYY.YYY.YYY.YYY: icmp: host ZZZ.ZZZ.ZZZ.ZZZ unreachable - admin prohibited
filter
0x0000   4500 0038 d52c 0000 f201 ca48 XXXX XXXX      E..8.,.....H.n..
0x0010   YYYY YYYY 030d 556e 0000 0000 4500 0047      ..#...Un....E..G
0x0020   1f00 0000 7e11 e17f 83d9 2306 ZZZZ ZZZZ      ....~.....#..=..
0x0030   0089 0035 0033 a693 93a6 4b71                ...5.3....Kq
```

Figure 9: Hexadecimal output using tcpdump

Figure 8 represents the output from tethereal. Bytes at addresses 0x003E and 0x003F represent the source port of the original datagram (0x0089 = 137 - NetBIOS Name Service) and bytes 0x0040 and 0x0041 destination port of original datagram (0x0035 = 53 - Domain Name Server).

Similarly, Figure 9 is an output from tcpdump. It outputs slightly differently by taking out of the hexadecimal output the link-level header. To see it, '-e' option was used and it is displayed at the top. In this case the source and destination ports are at bytes 0x0030-0x0031 and 0x0032-0x0033 respectively. What is significant is that the numbers are the same with both tools, 137 and 53 respectively, although SNORT was reporting both as 0.

To confirm this direct, 'hands-on' analysis, more advanced options were used to decode the packets to obtain more details directly from the tools. Ethereal and tcpdump produced again same results for source and destination ports of original datagram reported back with ICMP message.

Output from tethereal in much more readable format is presented in Figure 10. This is arguably most detailed view of a packet one can get with tools easily/freely available.

```
Frame 226 (74 bytes on wire, 74 bytes captured)
    Arrival Time: Aug 17, 2002 05:15:22.029533000
    Time delta from previous packet: 695.795558000 seconds
    Time relative to first packet: 231551.206677000 seconds
    Frame Number: 226
    Packet Length: 74 bytes
    Capture Length: 74 bytes
Ethernet II, Src: 00:04:9b:2f:e3:fc, Dst: 00:30:c1:0a:82:6b
    Destination: 00:30:c1:0a:82:6b (HEWLETT-_0a:82:6b)
    Source: 00:04:9b:2f:e3:fc (Cisco_2f:e3:fc)
    Type: IP (0x0800)
    Trailer: 93A64B71
Internet Protocol, Src Addr: XXX.XXX.XXX.XXX (XXX.XXX.XXX.XXX), Dst Addr:
YYY.YYY.YYY.YYY (YYY.YYY.YYY.YYY)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 56
    Identification: 0xd52c
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 242
    Protocol: ICMP (0x01)
    Header checksum: 0xca48 (correct)
    Source: XXX.XXX.XXX.XXX (XXX.XXX.XXX.XXX)
    Destination: YYY.YYY.YYY.YYY (YYY.YYY.YYY.YYY)
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 13 (Communication administratively filtered)
    Checksum: 0x556e (correct)
    Internet Protocol, Src Addr: YYY.YYY.YYY.YYY (YYY.YYY.YYY.YYY), Dst Addr:
ZZZ.ZZZ.ZZZ.ZZZ (ZZZ.ZZZ.ZZZ.ZZZ)
        Version: 4
        Header length: 20 bytes
```

```
        Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
            0000 00.. = Differentiated Services Codepoint: Default (0x00)
            .... ..0. = ECN-Capable Transport (ECT): 0
            .... ...0 = ECN-CE: 0
        Total Length: 71
        Identification: 0x1f00
        Flags: 0x00
            .0.. = Don't fragment: Not set
            ..0. = More fragments: Not set
        Fragment offset: 0
        Time to live: 126
        Protocol: UDP (0x11)
        Header checksum: 0xe17f (correct)
        Source: YYY.YYY.YYY.YYY (YYY.YYY.YYY.YYY)
        Destination: ZZZ.ZZZ.ZZZ.ZZZ (ZZZ.ZZZ.ZZZ.ZZZ)
    User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: domain (53)
        Source port: netbios-ns (137)
        Destination port: domain (53)
        Length: 51
        Checksum: 0xa693
```

Figure 10: Verbose output using tethereal

The most 'verbose' or detailed output from tcpdump is in Figure 11. It doesn't give as many details as ethereal, but all necessary details are clear.

```
05:15:22.029533 XXX.XXX.XXX.XXX > YYY.YYY.YYY.YYY: icmp: host ZZZ.ZZZ.ZZZ.ZZZ
unreachable - admin prohibited filter for YYY.YYY.YYY.YYY.137 >
ZZZ.ZZZ.ZZZ.ZZZ.53:  37798 updataA+$ [b2&3=0x4b71] [1537a] [1579q] [513n]
[11013au][|domain] (ttl 126, id 7936, len 71) (ttl 242, id 54572, len 56)
```

Figure 11: Most verbose output using tcpdump

4.3.2 Analysis of Collected 'traffic' Data

This part illustrates privacy implications arising from an analysis using ethereal on a full 'tcpdump' format log file.

Figure 12 is 'ethereal' output of one particular ftp session obtained from tcpdump data. It clearly shows that in a case of ftp connection all traffic flows unencrypted and is clearly visible to any person with access to the files. The same would apply for SMTP, POP and many other protocols regularly used on networks. Bold lines show user/password negotiation between two hosts on the network. Real addresses of the hosts were again replaced.

```
220 XXX.XXX.XXX.XXX FTP server (SunOS 5.8) ready.
USER antivir
331 Password required for antivir.
PASS McAfee
230 User antivir logged in.
TYPE A
```

```
200 Type set to A.
PORT YYY,YYY,YYY,YYY,4,23
200 PORT command successful.
LIST
150 ASCII data connection for /bin/ls (YYY.YYY.YYY.YYY,1047) (0 bytes).
226 ASCII Transfer complete.
TYPE I
200 Type set to I.
PORT YYY,YYY,YYY,YYY,4,24
200 PORT command successful.
SIZE update.ini
500 'SIZE update.ini': command not understood.
RETR update.ini
150 Binary data connection for update.ini (144.6.34.23,1048) (710 bytes).
226 Binary Transfer complete.
TYPE I
200 Type set to I.
PORT YYY,YYY,YYY,YYY,4,25
200 PORT command successful.
SIZE delta.ini
500 'SIZE delta.ini': command not understood.
RETR delta.ini
150 Binary data connection for delta.ini (YYY.YYY.YYY.YYY,1049) (1234 bytes).
226 Binary Transfer complete.
TYPE I
200 Type set to I.
PORT YYY,YYY,YYY,YYY,4,26
200 PORT command successful.
SIZE 42174218.upd
500 'SIZE 42174218.upd': command not understood.
RETR 42174218.upd
150 Binary data connection for 42174218.upd (YYY.YYY.YYY.YYY,1050) (118475
bytes).
226 Binary Transfer complete.
421 Timeout (900 seconds): closing control connection.
```

Figure 12: FTP session analysis using ethereal

Figure 13 shows that the above privacy concerns apply not only to communication between the two hosts, but also to transferred data. The figure shows what data have been transferred between the two hosts and subsequently captured by IDS after the command LIST was issued (underlined in Figure 12)

```
total 16808
drwxr-xr-x   2 antivir  staff       1536 Aug 16 09:00 .
drwxr-xr-x   5 root     other        512 Feb  2  2002 ..
-rw-------   1 antivir  staff       2674 Aug 14 09:36 .history
-rw-r--r--   1 antivir  staff        322 Jan 29  2002 .tcshrc
-rw-r--r--   1 antivir  staff      10171 May  5 02:04 42004201.upd
-rw-r--r--   1 antivir  staff     128208 May 10 02:04 42014202.upd
-rw-r--r--   1 antivir  staff     116751 May 16 18:36 42024203.upd
-rw-r--r--   1 antivir  staff     102355 May 23 08:15 42034204.upd
-rw-r--r--   1 antivir  staff     113660 May 31 02:04 42044205.upd
-rw-r--r--   1 antivir  staff     110231 Jun  7 02:10 42054206.upd
-rw-r--r--   1 antivir  staff      99892 Jun 15 02:06 42064207.upd
-rw-r--r--   1 antivir  staff     122500 Jun 21 02:13 42074208.upd
-rw-r--r--   1 antivir  staff     108621 Jun 28 02:08 42084209.upd
-rw-r--r--   1 antivir  staff     114676 Jul  4 14:16 42094210.upd
-rw-r--r--   1 antivir  staff     106037 Jul 11 10:18 42104211.upd
-rw-r--r--   1 antivir  staff      39037 Jul 16 14:17 42114212.upd
-rw-r--r--   1 antivir  staff     109103 Jul 18 15:05 42124213.upd
-rw-r--r--   1 antivir  staff     113554 Jul 25 03:18 42134214.upd
-rw-r--r--   1 antivir  staff     121067 Aug  1 08:31 42144215.upd
-rw-r--r--   1 antivir  staff      45615 Aug  3 15:04 42154216.upd
-rw-r--r--   1 antivir  staff     127155 Aug  8 15:09 42164217.upd
-rw-r--r--   1 antivir  staff     118475 Aug 15 15:13 42174218.upd
-rwx------   1 antivir  staff       2362 Jan 29  2002 antivirload
-rwx------   1 antivir  staff        781 May 22 12:10 checkupdate
-rw-r--r--   1 antivir  staff    2237545 Aug 15 15:08 dat-4218.zip
-rw-r--r--   1 antivir  staff       1234 Aug 15 15:13 delta.ini
-rw-r--r--   1 antivir  staff    4349267 Aug 15 15:13 sdat4218.exe
-rw-r--r--   1 antivir  staff        710 Aug 15 15:13 update.ini
```

Figure 13: FTP session (data) analysis using ethereal

4.4 Analysis and Discussion of Case A

One of the most significant findings from this two-month study was a bug in the reporting/alerting part of the SNORT system. As it has been shown in previous section (see 4.3.1), while the system correctly raised alarms on one particular rule set, the report it produced was not correct. From a network administrators' or security officers' point of view, this bug is not very significant because they would be able to identify a potential problem and then examine the captured network packets using tcpdump and/or ethereal tools to

provide the correct information. However, from a forensic computing perspective this bug could hamper the admissibility and/or validity of evidence derived from the captured data. The discrepancy between text of the alert and real data (illustrated in Figure 7 - Figure 11), supports the view that IDS' are problematic as tools for the collection of forensic computing data sets (Broucek & Turner, 2002a, 2002c; Sommer, 1998b, 1999). This bug was fixed in SNORT version 1.9.0; however, another bug, that time in formatting alert output files was discovered. The new bug prevented some of the tools developed for SNORT log files manipulation (e.g. SnortSnarf) from correct operation.

The two months of monitoring the server provided large amounts of data. As a matter of the fact, due to storage limitations full 'tcpdump' format log file could not be collected for the whole period. The study has illustrated that rule sets and configuration files have to be highly customised and continuously fine-tuned. Decisions about 'trusted hosts' have to be made often on the basis of partial knowledge. It has further been shown that many hosts that should potentially be granted 'trusted status' due to the service provided cannot be granted such a status due to the nature of other problems, for example with DNS lookups. The data reveals that attempted attacks were made both from inside the University Network and the Internet. The server was probed not only on ports that have been made available and known (the server was advertised on University's website), but also on ports that were not readily 'visible' to users of the University network or the Internet. On ports 80 and 443, probes mainly attempted to exploit known vulnerabilities in Microsoft IIS server. The persistence of these repeated attempts suggests that many of these attacks were automated and the scripts not written very well. It is questionable why a 'would be attacker' risks being discovered by repeating these attacks on a system that is not susceptible to such attacks. This is especially the case given that it is possible for them to identify first the server software and then make decisions about whether to attempt an attack. While external attacks from the Internet were only experienced on TCP ports 80 and 443 due to firewall restrictions, internal attempts were much broader. Again, some of the attacks were

completely futile for the attacker but provided valuable data for a forensic investigator wishing to identify the location or intention of the attacker.

Using the IDS system can help to protect the web server against malicious attacks. However, the amount of false positive alarms, fine tuning and alert monitoring required definitely proves that properly trained security personnel/system administrator needs to be available to monitor such a system continuously. It has proved useful to collect all the traffic in the 'tcpdump' format. This is particularly the case because it opens up the possibility of the data later being examined by other tools, in this case ethereal and tcpdump. Clearly, it is very hard, if not impossible, to rule out all of the false positive alarms based only on information obtained from alert file produced by SNORT. However, with careful analysis of the whole connection it is possible to prove beyond a reasonable doubt that the traffic is either malicious or false positive alarm. However, even such data would have only limited value in prosecuting potential attackers as the information provided in the 'tcpdump' format file is limited to the TCP/IP packet load. Additional information needs to be obtained from other sources – log files, route tracing etc.

As an example of this point (see 4.3.1), one particular repeating alert in the data collected during the study highlights that such data does not provide sufficient information for tracking back and tracing the attacker or source of the alarms. In this case, an attack exploiting vulnerabilities of NetBIOS name service and Domain Name Service on UDP ports 137 and 53 appeared to be initiated inside the University network. This triggered 'ICMP Destination Unreachable' alerts. It appeared that the 'ICMP Destination Unreachable' packets were being sent to local network due to a host on local network attempting this particular attack. The TCP/IP address of the 'offending' host pointed to a Hewlett-Packard printer located on local network. However, checking the firewall log files and firewall set up proved that the attack was not initiated inside of the University's network. The conclusion reached was that the attacker, somewhere on the Internet, was using a 'decoy' technique and the server with IDS was unlucky enough to be in the 'decoy' address space. When

the attacker tried to attack the site that had port 53 blocked, local network was receiving a broadcast ICMP message.

To be completely sure that there was not something going wrong, the host supposedly causing the messages that generated the alarms was shut down. The alerts continued to be triggered in nearly regular 12 hours intervals. Administrators of the router sending the ICMP messages were contacted and asked for help in locating the attacker. While they did not respond, the messages stopped coming after several days, even with local host back on-line. After some time, the messages started to come yet again, from a slightly different router, however at the same domain. Furthermore, as described previously and analysed in section 4.3.1, this particular alert message suffered from a bug in the used version of SNORT.

This experiment also confirms that SNORT NIDS is not capable of protecting against attacks conducted over the secure socket layer (SSL). The only way of detecting these attacks is to examine carefully server log files. The encrypted traffic simply does not provide patterns that could be used for creating rules for attacks run through SSL. These results suggest that it might be highly desirable to develop a module for Apache server software that would provide 'application based' intrusion detection. With the availability of rule sets (either from SNORT or any other public domain source), application programming interface (API) and in particular the greater modularity of Apache version 2.x this should be a relatively straightforward module to develop.

Finally, these findings support calls being made by governments and law enforcement agencies for continuous monitoring of network traffic. However, to protect individuals' privacy it is necessary to develop techniques for this monitoring that will not interfere with the individual's rights (Biskup & Flegel, 2000a, 2000b, 2000c; Kvarnström, et al., 2000; Lundin, 2000; Lundin & Jonsson, 1999a; Sobirey, et al., 1997).

4.5 Preliminary Findings for Case A

By adopting a forensic computing perspective this study has confirmed concerns raised about the suitability of Intrusion Detection Systems as sources for evidence acquisition (Sommer, 1998b, 1999). Specifically, two main concerns previously raised by Broucek & Turner (2002a, 2002c) have been validated by this case study:

- IDS systems may collect only a partial data set – it has been shown that data collected by SNORT were not sufficient to track and trace attackers and that the data collected in the case of encrypted communication using SSL had no value in this regard;
- The data sets collected may be flawed, erroneous or already have been tampered with – it has been shown that even with significant fine-tuning SNORT produced numerous false positive alerts and/or wrongly identified the source of attacks.

More significantly, the case study has highlighted that from a legal perspective IDS, the data they produce and how that data is analysed pose numerous challenges for those interested in evidence acquisition that produces legally admissible evidence. In particular, even where data has been captured, the process of its technical analysis may invalidate it in terms of legal admissibility by 'tampering' with the evidence. Considering the underlying problem of unclear and ambiguous definitions, it is then imperative that in approaching the collection of forensic evidence that there is awareness of some key principles: minimise handling of the original data set; account for any change; comply with the rules of evidence; and, do not exceed your knowledge (McKemmish, 1999).

The case study has also highlighted that the 'collect everything' approach is highly desirable but has severe limitations and implications:

- Section 4.3.2 provides an analysis of one FTP session. It shows how much information investigators with access to such data can obtain from it. Clear

text transactions are easily visible and, source and destination hosts are easily identifiable. If SNORT was deployed in its usual configuration as a network IDS, it would collect large amount of data that could clearly violate the privacy rights of academics, students and other network and Internet users.

- More generally, the log files are huge in size even where SNORT is monitoring only one rather minor and uninteresting web server. All alerts were collected into one 'flat' file and several binary 'tcpdump' files were also collected. The longest time period collected into one file was about 193 hours – during which 664848 packets were captured and the size of the file was 157MB. To read this file into Ethereal with only MAC and transport name resolutions switched on took 3 minutes and 50 seconds on a Pentium IV 1.7GHz system running RedHat Linux 8.0. It took even longer on Sun Ultra 5 running Solaris 8 that was used for these analyses. Requests for filtering or 'following TCP stream' took even longer. This clearly demonstrates that in a case of serious deployment, large storage space is needed and that an effective log rotation system has to be developed to allow quick and timely analysis.

The study also confirms that Intrusion Detection Systems can play an important role in protecting Information Systems Infrastructure. However, to be effective they require attention of highly trained security personnel/system administrators in:

- Regular monitoring and analysing alerts and other log files and acting upon them;
- Continuous fine-tuning the configuration files and rule sets for the ever changing IS environment; and
- Regular updating the rule sets to accommodate newly discovered threats.

This case confirms that Intrusion Detection Systems face significant challenges as part of the armoury of computer security. Research and development in this area continues working on solutions for these challenges (see 2.4.2). However,

this chapter also reveals that these developments, aimed at responding to the challenges faced by computer security, tend to occur without any consideration of possible knock-on effects for other areas. This raises the concern that the 'clever' solutions being developed may end up adversely impacting on solutions being developed in other areas, and impede forensic investigations and the acquisition of digital evidence.

4.6 Summary Reflection on the Chapter

This chapter provides analysis of Case A. The analysis involves descriptive statistical analysis of network data and reveals problems with the validity and quality of the data. The results of the analysis show that data collected by SNORT are not sufficient to track and trace the sources of the attacks. The analysis also reveals that the data sets collected may be flawed, erroneous or already have been tampered with. Despite significant fine tuning, SNORT continued to generate numerous false positive alerts and/or wrongly identified sources of attacks. This case highlights that intrusion detection systems can play an important role in protecting information systems infrastructure, but to be effective they require the attention of highly trained security personnel/system administrators. These personnel also need to engage in regular monitoring and analysis of alerts and other log files, and to ensure regular updating of the rule sets used by these systems.

5 Data Analysis Case B – MP3[8]

> ***Question**: "What are the problems that you as an individual face?"*
> ***Answer (laughing)**: "Too numerous to mention – for example; investigator requests a print out of the hard drive so that he/she can look at the contents..." (Detective Sergeant Paul Wright, City of London Police, UK, interviewed at DFF 2007, Prague)*

5.1 Introduction

The case in the Federal Court of Australia involving Sony Music Entertainment (Australia) Limited, Universal Music Australia Pty Limited and EMI Music Australia Pty Limited (the applicants) and three Australian Universities – the University of Tasmania, University of Melbourne and University of Sydney (the respondents) generated considerable public interest and debate. Unfortunately, much of the debate and conjecture around the case had been misplaced due to incorrect reporting in many media reports that suggested the case was about the Universities being sued for copyright infringement. There were also other media reports suggesting eleven Australian Universities were involved in the 'MP3 Piracy Case' as it has alternatively been called ("Aust unis in court over file-swapping," 2003; Lamount, 2003; Morgan, 2003; Rose, 2003). If this was the situation, it is indeed noting that of all the Australian Universities approached only these three offered any resistance to initial requests by the Music Industry for access to their digital files and networks.

---

[8] Please note some of the material presented in this chapter has been adapted from materials first published in the following peer reviewed publications:

Broucek, V., Turner, P., & Frings, S. (2005). Music piracy, universities and the Australian Federal Court: Issues for forensic computing specialists. *Computer Law & Security Report, 21*(1), 30-37.

Broucek, V., Frings, S., & Turner, P. (2003). The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists. In C. Valli & M. Warren (Eds.), *1st Australian Computer, Network & Information Forensics Conference*. Perth, WA, Australia.

In reality this Federal Court case was procedural in nature and involved the Music Industry applicants seeking a 'discovery ruling' against the three Universities involved ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003)," 2003; Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 724 (18 July 2003)," 2003; Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003)," 2003; Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 929 (4 September 2003)," 2003). Next section reviews the case, identifies issues and challenges and draws out challenges posed for legal environments.

5.2 Descriptive Analysis of Case B

On January 23, 2003 the Australian Record Industry Association (ARIA) released information suggesting that the industry was suffering significant losses in earnings due to on-line piracy and that the industry was determined to combat these activities ("Online piracy hurts 2002 music sales: ARIA," 2003). While peer-to-peer (P2P) networks were not specifically targeted in this case, ARIA also cited its US counterpart, the Record Industry Association of America (RIAA), ongoing war with peer-to-peer networks and their users.

At around the same time, three Australian Universities (University of Tasmania, University of Melbourne and University of Sydney) were approached by members of the Australian music industry (Sony Music Entertainment (Australia) Limited, Universal Music Australia Pty Limited and EMI Music Australia Pty Limited) and requested to preserve digital evidence on these Universities systems of the distribution of MP3s by students and staff at these Universities. In the case of the University of Tasmania, music industry legal representatives sent an e-mail regarding one particular web site that was allegedly hosting copyright MP3 files. These were found using a Google™ search. Subsequently, these machines were copied as requested and stored in the fire proof safe in late January 2003. From forensic computing view, it is important to note that due to the nature of the request and lack of training and

forensic readiness, the copies were made using built in *ufsdump* backup command instead of more appropriate binary copy that would be obtained by using another built in command (*dd*).

These MP3s and distribution activities were being categorised by the music industry as potentially constituting breaches of copyright laws. Subsequent to this request to the Universities, the members of the music industry further requested access to this evidence for discovery. In response, the three Universities concerned refused to provide this access. At the University of Tasmania, this occurred in the context of on-going concerns about privacy in contracts with external research collaboration projects.

On February 18, 2003 these music industry members (applicants) launched legal proceedings against the respondents in order to gain access to the evidence preserved by the respondents at their request. The basis of the legal proceedings were procedural with applicants seeking a right of access to the preserved evidence in order to conduct discovery investigations that could possibly lead to identification of person(s) involved in copyright infringements who would then be acted against in subsequent litigation.

At the initial hearing on February 18, 2003 the case was adjourned and orders made to the respondents to preserve the data. Immediately, the case and initial ruling created outrage amongst academics, students and civil liberty groups who viewed this as the beginnings of a major assault on the privacy of individuals. Indeed, the demands made by the applicants at the initial hearing were labelled as 'witch-hunting' and using students and Australian universities as 'scapegoats'. A series of questions were raised, including as to whether the Universities should be forced into the role of policing and/or taking responsibility for the on-line activities of their staff and students (Morgan, 2003).

Subsequently, on May 30, 2003, after a number of further court sessions and out-of-court attempts to find a mutually acceptable solution, the presiding judge, Justice Tamberlin, made his decision in favour of applicants ("Sony

Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003)," 2003) and on July 18, 2003 ordered the respondents to hand over the evidence to the applicants and their forensic expert for further investigation ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 724 (18 July 2003)," 2003). While the legal right of the court to make this ruling cannot be doubted, it raises serious questions about the courts understanding of the nature of the digital evidence in question. Significantly, on July 29, 2003 ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003)," 2003) Justice Tamberlin also ordered the respondents to bear the cost of the discovery process and in determining which data to be handed over, argued that 'deleted files are equal to overwritten files', when one of the respondents pointed out that the backup tapes in question had accidentally been overwritten and therefore did not have any forensic value for the applicants (Pearce, 2003). Again, this reveals a worrying lack of understanding of the technical nature of digital logs and data storage. While there may have been a 'suspicion over the accidental overwriting', from a technical perspective it was inappropriate to consider overwritten backup tapes as part of the evidence. Subsequently, this ruling was used by the Music Mndustry in mounting 'a possible contempt of court' challenge against the University of Sydney. This challenge resulted in a small but significant victory for the respondents, as it was dismissed and the applicants ordered to pay cost ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 929 (4 September 2003)," 2003).

5.2.1 Subject of Dispute

Initially, the three involved Universities did not agree with the request for the discovery at all. However, as the case has evolved these respondents were forced to find additional arguments to oppose the arguments used as the basis for the requests made by the applicants. The respondents' initial opposition was primarily based on the premise that excessive access to this data could lead to breaches of privacy and intellectual property law covering aspects of the data held. They had, however, been willing from the outset to provide some digital

evidence to the applicants, providing that this evidence was collected by respondents and then handed onto the applicants. Several offers of this kind were made; however, the applicants were dissatisfied with the amount of data and discovery offered.

From the beginning the applicants demanded the rights to conduct full forensic investigation of the preserved data. It should be noted that the vast majority of the data in question contains (or contained) information on the on-line activities of thousands of 'presumably innocent' users and not just data on users that were alleged to be guilty of illegal practices. However, what is certain is that the most of this data related to activities pertaining to personal, confidential and commercial activities of the Universities' staff and students as part of their research, teaching and commercial activities. In this context, the judgement in this case provided unprecedented access to huge amounts of potentially highly sensitive data because of a suspicion that some of it might contain evidence of illegal practices. Unfortunately, the judgement did not, however, provided this data access to an independent third party (for example, an external forensic investigation team) but rather to the very same groups who have 'pointed the finger' in the first place. These applicants were then allowed to 'mine' this data in search of what they themselves deem 'illegal practices'. Quite apart from the intrusion into the data of thousands of 'presumably innocent' users, issues of data tampering/manipulation (except where MD5 check-sums were calculated and stored by respondents), breaches of privacy, commercial dealings, intellectual property were all only protected by confidentiality provisions placed on the applicants.

As a result of this case and concerns over the issues at stake in such 'data hand-overs', the majority of Australian Universities have now started to conduct their own forensic investigations. Numerous Universities have embarked on 'scare campaigns', reminding staff and students about importance of copyright protection and possible outcomes for breaches. They have also engaged in network traffic monitoring and scanning computers for MP3 files often without knowledge of the users (Nelson, 2003a). Many of these searches are being

conducted in a manner that further creates dangerous precedents and fears over violations of privacy and academic freedoms. In many instances the techniques employed were very amateur. For example, in one instance computers and servers were searched using the *find* command with *.mp* mask[9]. Searches of this type clearly produce numerous false positives and identify files that do not have anything to do with audio or video recordings (e.g. files with extension *.mpp that belong to Microsoft Project program). Furthermore, many audio card drivers and software themselves contain sample MP3 format files (e.g. the Microsoft Software Development Kit (MSDK) contains MP3 and mpg samples). As a consequence, many users were harassed by overly active and poorly instructed network and computer administrators and forced to delete legitimate files in a fear of possible copyright law breaches.

Combined, this case and the responses of Australian Universities resulted in making many network administrators at the Universities afraid to report suspected computer misuse of their systems. This is because they are either afraid that they will be held responsible or that they will have to conduct or be involved in forensic investigation for which they feel unqualified.[10]

5.3 Complexity of Issues and Implications for Stakeholders

This case and the responses of its participants highlight a number of issues worthy of consideration. Firstly, from the users' perspective, education about appropriate behaviour in digital environments is still a major issue (Broucek & Turner, 2003a). The majority of people are not aware of the legality of creating MP3 copies from their CDs and are not aware that 'state-swapping' is illegal in

[9] It should be noted that these techniques were only used as initial indicators; however anecdotal evidence of the author is that University of Tasmania conducted similar searchers as recently as in 2009.

[10] Also resource requirements in SW, HW and HR.

Australia (Nelson, 2003b)[11]. This is perhaps partly because the market is flooded with MP3 players and that some operating systems now come with 'ripping software'. There is therefore an urgent need for improved user education (Broucek & Turner, 2003a).

Secondly, it is noticeable that none of the Universities involved in the case were prepared for the initial request for the preservation of the evidence. The initial collection was conducted by the Universities network and systems administrators, without any training in forensic procedures as is evidenced by the nature of the evidence collection and storage processes used. File level copies of file systems were made to CD-ROMs or standard backup procedures were used to preserve the evidence. For example, in the case of University of Tasmania, the standard backup tapes created were subject to the discovery and the evidence from one particular computer where allegedly illegal MP3 files were held was collected by standard UNIX backup command, *ufsdump*.

While these tapes may contain the necessary evidence of files being stored on the computers, in the opinion of the author, this evidence will be of very low value in a subsequent legal proceedings as it was not collected using binary copies and neither the chain of custody or rules of evidence were followed (Broucek & Turner, 2001a, 2002a, 2002c, 2003b).

Thirdly, the approach adopted in the case is potentially short-sighted in that it is probable that many University users will now proceed to encrypt all of their communications to impede subsequent 'snooping'[12]. Overall this highlights a

---

[11] This has changed since the original analysis and it is now legal to create copies of legally purchased CD-ROMs for own use on personally owned devices. It is important to notice the 'personally owned', because it is still illegal, for example, to play legally purchased MP3 files on computer owned by company or university.

[12] i.e. PGP or SSL with keys 1024 or greater. Of course, it can be argued that pushing the introduction of encryption would inhibit the availability of illegal material because most P2P networking is not possible or hampered by this technique.

lack of 'forensic readiness' on the part of all participants and the need for set procedures, covering all possible variants of investigations involving digital evidence to reveal any criminal, illegal or other inappropriate behaviours. Forensic procedures should be in place to protect organisations and in this context the next section briefly examines the CTOSE framework that has made a significant contribution to the development of a generic process model and advisory tools for conducting forensic investigations (Frings, Stanisic-Petrovic, & Urry, 2003; Urry & Mitchison, 2003).

5.4 Preliminary Findings for Case B

In the post September 11th era, the threat of global terrorism has stimulated significant extensions being given to law enforcement agencies. These powers have increasingly been extended into the digital domain through legislative developments at national and international levels e.g. Australian Cyber-Crime Act 2001, 'Patriot Act' in USA, and on-going legislative discussions within the European Union, Council of Europe and the USA. In conjunction with these legislative developments efforts were made to generate practical tool-kits for investigating computer misuse and e-crime in a manner that will produce legally admissible evidence e.g. CTOSE (Cyber Crime Tools for On-line Search for Evidence) (Broucek & Turner, 2004a; Broucek, et al., 2005). However, as was discussed above, while these efforts are laudable, numerous questions on the legal admissibility, legal validity/weight, chain of evidence and chain of custody of digital evidence continue to make problematic the development of legal responses to illegal or inappropriate on-line behaviours (Broucek & Turner, 2002a, 2002c).

More significantly, in the context of the discussions here, even where digital evidence is available and has been accepted as admissible, critical issues have emerged over the understanding of the courts on the nature of this evidence. For example, the MP3 piracy case involving representatives from the Australian music industry and three Australian Universities in a dispute over the distribution of MP3s by students and staff at the Universities reveals a

"*worrying lack of comprehension of the technical nature of digital logs and data storage*" (Broucek, Frings, & Turner, 2003; Broucek & Turner, 2004a; Broucek, et al., 2005). More specifically, this lack of understanding resulted in the provision of access to data sets that contained information on the on-line activities of thousands of presumably innocent users and not just data on those alleged to be guilty of computer misuse. This provision of unprecedented access to huge amounts of potentially sensitive data pertaining to the personal, confidential and commercial activities of innocent users is clearly of concern. This is especially the case where access to the data was not handed over to an independent third party but rather to the applicants in the case.

From a forensic computing perspective, not only does the case reveal a lack of forensic readiness on the part of the courts, the applicants and defendants, it also raises questions about the supposed expertise of the forensic experts used in the case. However, quite apart from the consequences of these circumstances in the specific case, other important questions are raised in relation to the potential consequences of these types of approaches being displayed by courts. Indeed, as has been argued elsewhere, the approach adopted by the Australian Federal Court and the applicants in the case "*is short-sighted and may back-fire on the music industry's desire to crack-down on piracy*". This is because it is probable that many users will now proceed to encrypt all their communications to impede subsequent 'snooping'. The case has also made "*many network administrators in Universities reticent about reporting on suspected computer misuse of their systems*". This is because they are either afraid that they will be held responsible or that they will have to conduct or be involved in e-forensic investigations for which they feel unqualified (Broucek, et al., 2003; Broucek & Turner, 2004a; Broucek, et al., 2005). The case may also influence the way in which organisations 'back-up' their systems and how long they retain this data. Combined, all of these factors are likely to make collection, investigation, generation and presentation of digital evidence of illegal or inappropriate on-line behaviours more difficult.

More broadly, as the law continues to generate responses to the challenges faced, it is clear that there are strong inter-relationships with public perceptions and changing end-user and organisational behaviours for on-line environments. Critically, there is the danger that if legal responses do not show sensitivity towards these inter-relationships end-users and organisations seeking to protect themselves will behave in ways that will problematise the acquisition of digital evidence and potentially reduce overall system e-security.

This case confirms that the legal area faces significant challenges. This area continues to work on 'technology neutral' solutions for these challenges (see 2.5.1). However, this chapter also reveals that these developments, aimed at responding to the challenges faced by the legal area, are hampered by tradition bound legal process and problematic analogies between analogue and digital domains. This is additionally hampered by the problems in defining forensic computing and even digital evidence as it has been presented in section 2.3.

5.5 Summary Reflection on the Chapter

This chapter has reviewed and examined an Australian Federal Court case between the Music Industry and three Australian Universities. From a forensic computing perspective the case reveals the strong and urgent need for development of standard procedures for collecting and preserving the digital evidence and the need for greater 'forensic readiness' whether dealing with criminal, civil or inappropriate on-line behaviours. While it remains unclear what the end result of the 'discovery' activities of the music industry was, it is evident that the case also had a number of worrying implications for individual users' privacy and the confidentiality of data held within institutions.

6 Data analysis Case C - CTOSE[13]

"All investigations are reactive in that an event must occur (fraud) before the investigation can take place; there is little scope to be pro-active in this role. The time frame for investigations, by their very nature, is on average about 4 years, but bear in mind that we will be reviewing many millions of items to construct the case" (Keith Foggon, head of the digital forensics unit, Serious Fraud Office, UK).

6.1 Introduction

With the increasing incidence of computer misuse and e-crime, public and private sector organisations have increasingly sought ways to respond. These responses have included increased e-security precautions, computer usage policies, monitoring and education as well as in some instances the establishment and deployment of forensic computing investigation teams. Whilst these responses are sensible and understandable, in some cases their implementation has had unforeseen results that have actually impaired the overall security of the organisations concerned. Partly, this result from draconian measures imposed on users of the systems and partly from a general lack of awareness amongst most users of the implications for e-security of their on-line usage behaviours.

In this context, this chapter provides an analysis of EU funded CTOSE project. This project received significant funding and attention across Europe and many

---

[13] Please note some of the material presented in this chapter has been adapted from materials first published in the following peer reviewed publications:

Broucek, V., Turner, P., & Frings, S. (2005). Music piracy, universities and the Australian Federal Court: Issues for forensic computing specialists. *Computer Law & Security Report, 21*(1), 30-37.

Broucek, V., Frings, S., & Turner, P. (2003). The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists. In C. Valli & M. Warren (Eds.), *1st Australian Computer, Network & Information Forensics Conference*. Perth, WA, Australia.

major institutions were involved in it. The results were considered to be very positive and it was expected that the CTOSE solution would become the 'de-facto' standard across Europe. This methodology has been taken up by various users, but has also been adapted by them to suit their specific needs. Some of the elements of the project have also been adopted commercially including by the Bank of Scotland (see below, forensic readiness section 6.3) or incorporated into government policies (e.g. UK).

Following the conclusion of the CTOSE project, some of the partners in the original project established the CTOSE Foundation with the aim of the commercialisation of the project results. Unfortunately, the initial excitement did not produce the expected results and the foundation ceased to operate after less than two years.

However, it is important to note that the original aim of the CTOSE project (and its funding by EU) was not to produce commercial products and as such the project was very successful.

In terms of key lessons learned from the CTOSE project, one of the two project managers of the CTOSE project has stated that the most important lesson learnt from the project was the fact that

> *"the path from methodology to operational methodology is a long and expensive one" (Mitchison, 2009).*

In one sense, the CTOSE project was a victim of its own success in that it achieved a great deal but ended up trying to do too much in the short time frame provided by the funding (3 years). These challenges however did not become evident, even to the project's partners, until the project was finished and the CTOSE foundation established.

Some of the reasons for failure of the commercialisation stage (CTOSE Foundation) that need to be considered were:

- Lack of management/commercialisation skills amongst the key researchers;

- Lack of real proof that the model was practicable and would work outside of the demonstration projects in a range of organisational settings and contexts;
- Despite commercial partners in the project, it was driven by academic researchers focused on questions of methodology rather than commercial potential; and,
- Although there was great input from experts in the field there was a failure to adequately address the multi-dimensional aspects of electronic evidence in a manner that effectively balanced all interests.

6.2 CTOSE Development

The CTOSE (Cyber Tools On-Line Search for Evidence) project aimed at developing and testing methodology suitable for collection of digital evidence in various environments and for various purposes. The primary motivation behind the establishment of the CTOSE project was to improve the ability of companies to respond to computer misuse incidents. The significant benefit of this project is that it did not limit itself to criminal investigation, but focused also on other avenues where forensic computing could possibly be used.

The project was funded under the 5th Framework Programme and brought together various players, namely:

- University of Namur, Belgium;
- St Andrews University, UK;
- Fraunhofer, Institute Arbeitswirtschaft und Organisation, Stuttgart, Germany;
- The Joint Research Centre (JRC), Italy;
- QuinetiQ, UK; and
- Alcatel, France.

This has been complemented by a network of user focus groups under the leadership of JRC. This network included representatives from the legal, financial, law enforcement and IT industry. Author of this thesis had the

privilege to take part in several focus groups, including attendance and presentation at the CTOSE 2003 Conference in Namur Belgium (Broucek & Turner, 2003b, 2004b).

6.3 CTOSE Outputs

One of the first tasks that CTOSE conducted was an attempt to formalise the definition of digital evidence. During the initial interview and questionnaire phase with key stakeholders in the Special Interest Groups (SIG), the following types of digital and/or electronic evidence were determined to be of importance in 'proving' a particular case. Members of the SIGs were asked to provide examples of electronic evidence during interviews and in questionnaires. Based on their answers, the following list of types of electronic evidence was compiled:

- Log files – this includes server logs, ISP logs, IDS log files etc;
- Core files;
- Copies of hard disks including all log files;
- E-mails;
- Network dumps; and
- Network traffic samples and grabs.

It was noted that such electronic evidence should satisfy two legal tests:

- Admissibility; and
- Weight.

On the basis of this list a project deliverable was prepared. This deliverable was the Electronic Evidence Specification Model (EESM). Figure 14 shows the model.

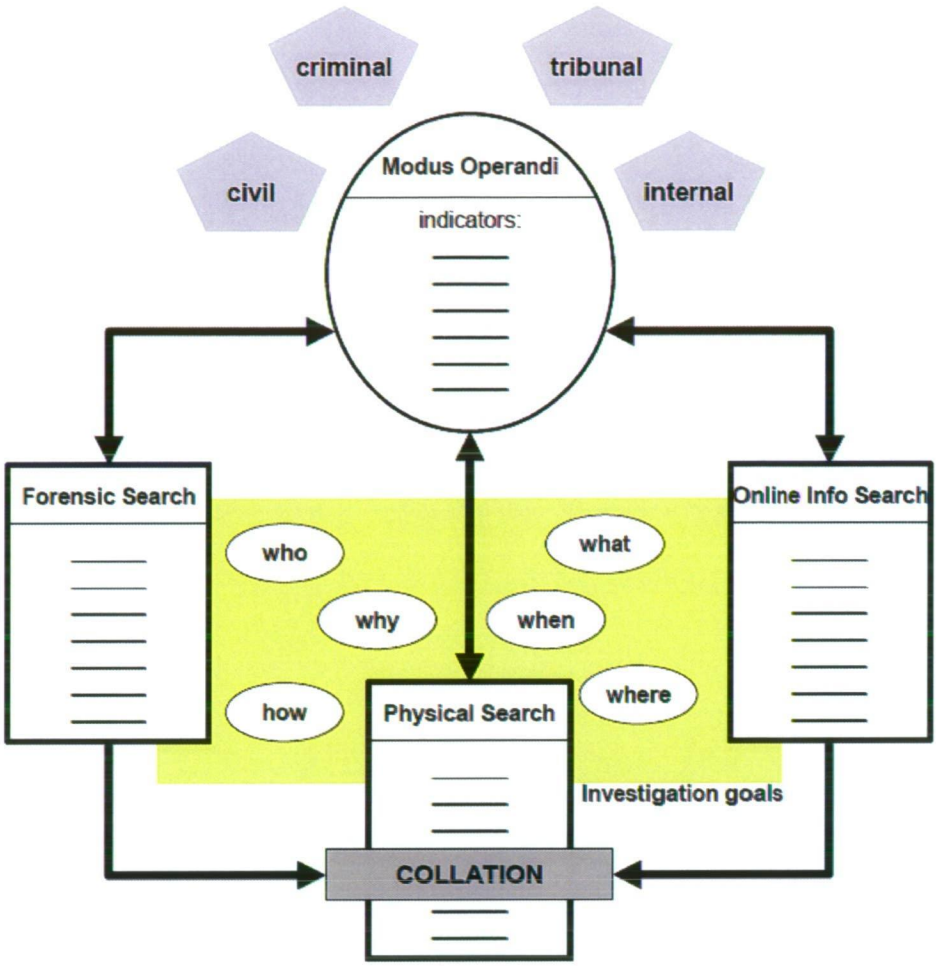


Figure 14: Electronic Evidence Specification Model (EESM)

This model clearly emphasizes the legal and organisational dimensions of digital evidence acquisition and presentation. It provides a useful schematic of the processes involved and draws attention to some of the inter-relationships involved in these processes as they relate to evidence specification. Unfortunately, the model appears to have been generated on the basis of a consideration of only legal dimensions. That the project did not use any of the previously mentioned definitions (see section 2.3) and developed its own approach again highlights how definitional ambiguity can impact on responses to criminal, illegal or other inappropriate on-line behaviours.

More specifically, the lack of incorporation of any other definitions of digital evidence may have impacted on the later acceptance or adoption of the project outputs in the wider community. Critically, the absence of any direct or explicit acknowledgement of the definitional ambiguity around digital evidence and the challenges that this poses for the generation of a coherent model is disappointing. From a practical perspective, working with the project's SIG clearly made the production of the above model easier but the dominance of the 'legal' perspective ended up leading to a model that does not adequately address the challenges of the multi-dimensional aspects of forensic computing and displays limited consideration of the technical aspects. This perpetuation of the divide between legal and technical is unhelpful and again contributes to the foci of this thesis

Subsequently, the project has developed a methodology that aims to provide a consistent approach for identifying, preserving, analysing and presenting digital evidence.

In this regard, the CTOSE project began by developing a reference process model resembling organisational, technical and legal guidelines on how a company should proceed when computer misuse occurs. The focus of the model is on the acquisition of digital evidence and on how it is to be collected, conserved and analysed in a manner that will be legally admissible should court proceedings be instigated. Figure 15 illustrates how this reference model links to a detailed examination of technical, legal and presentational requirements, which in-turn link to the project software demonstrator.

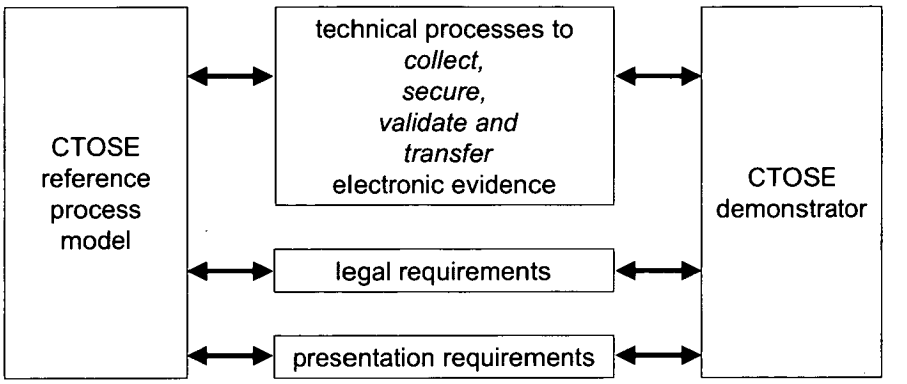


Figure 15: CTOSE Project

The CTOSE reference process model is composed of five phases: preparation, running, assessment, investigation and learning phases. It articulates the flow of actions and decisions that have to be considered or executed in the case of an investigation of computer misuse. Moreover, additional detailed information is provided that directly addresses the investigator roles and the necessary skills, checklists, references to documents and tools, and legal advice that are required to support the action or decision in each step (see Figure 16). By providing this information the CTOSE reference model aims to support user through a checklist approach that can be consulted prior to, during and at the conclusion of an investigation of an IT incident. This checklist also supports investigators by addressing in detail the technical information that law enforcement agencies may require from the individual and/or organisation involved. The model also aims to support the optimisation of communication between the two parties.

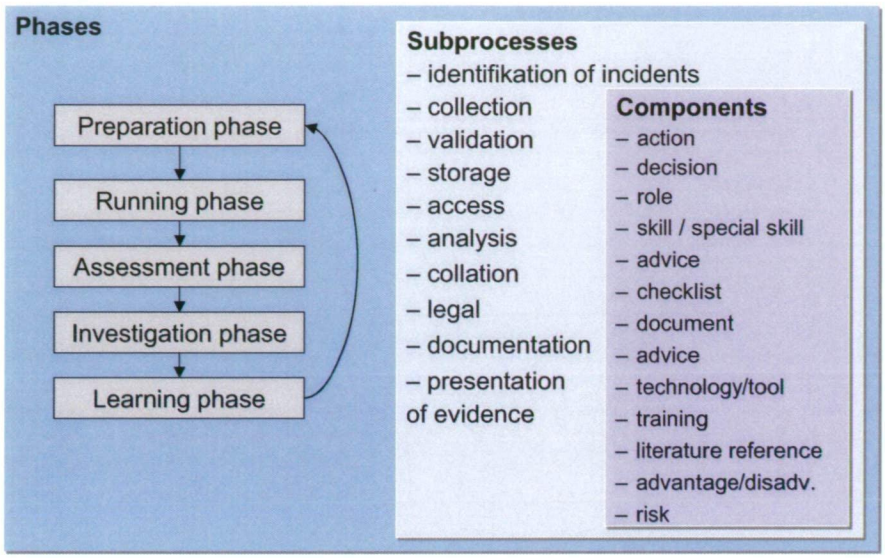


Figure 16: CTOSE Phases of Response

Significantly, the CTOSE project emphasizes the preparation phase, also referred to as 'Forensic Readiness', because IT security measures critical to the whole process are defined and implemented in this phase. For example, this phase includes technical aspects like implementing a firewall and/or an intrusion detection system and assures that qualified staff is present to administer the systems and evaluate their logging.

This was arguably the most successful part of the project. Two of the CTOSE member teams (QinetiQ and Alcatel) further developed it and now offer it as a commercial service. Furthermore, it has now been incorporated into the UK government's security policy (see http://www.cabinetoffice.gov.uk/spf.aspx).

While the majority of the rest of the reference model concentrate on details of the running, assessment and investigation phases the model also acknowledges the importance of having a feedback loop to capture insights from concluded investigations to further strengthened and enhance the approach of an individual and/or organisation. This final phase is referred as the learning phase.

Although in Figure 16 above the learning phase is presented as being the last phase, in fact the CTOSE approach emphasizes the importance of capturing

learning and insights during each phase as well as in a dedicated learning phase at the end of each and every investigation or even test run.

The aim of this learning phase was to reflect on the achieved results and problems faced and where possible adjust or enhance any parts of the investigation process including internal methodology, the software tools, the recordings.

In particular, the learning phase contains a series of questions that individuals and/or organisations are encouraged to consider:

- Was everything correctly and completely documented?
- Were the people involved qualified enough for given task?
- Was the process correct or is there need to modify or update it?
- Were all contact people the correct ones?
- Was there anything else that could be improved for next time?

Following informal communication with the former leaders of the CTOSE project to obtain some additional information about the project and in particular the learning phase, it is useful to note that a number of them recognised the challenges of 'doing this phase well'. It was acknowledged that organisational context, individual skill sets and the time-frames of the investigation directly impacted on the ability of organisations to respond to any learning. Additionally, it was acknowledged that in some instances organisations found it difficult to even enter the learning phase formally.

> *"In practice the project - even in the demonstrators - never got as far as doing that, because we were busy setting up the initial approach. But in real-life uses of parts of the project methodology, they did indeed do that."(Mitchison, 2009)*

6.3.1 The Software Prototypes

As a consequence of the complexity of the process reference model (see Figure 17 for a small fragment of it), it was decided that the CTOSE project would

develop an electronic version. Sandra Frings (Fraunhofer, Institute Arbeitswirtschaft und Organisation, Stuttgart, Germany) who was the principal author of the model, admitted in private conversation with author of this thesis that if printed in reasonably readable format, the model would cover floor of large lecture theatre...

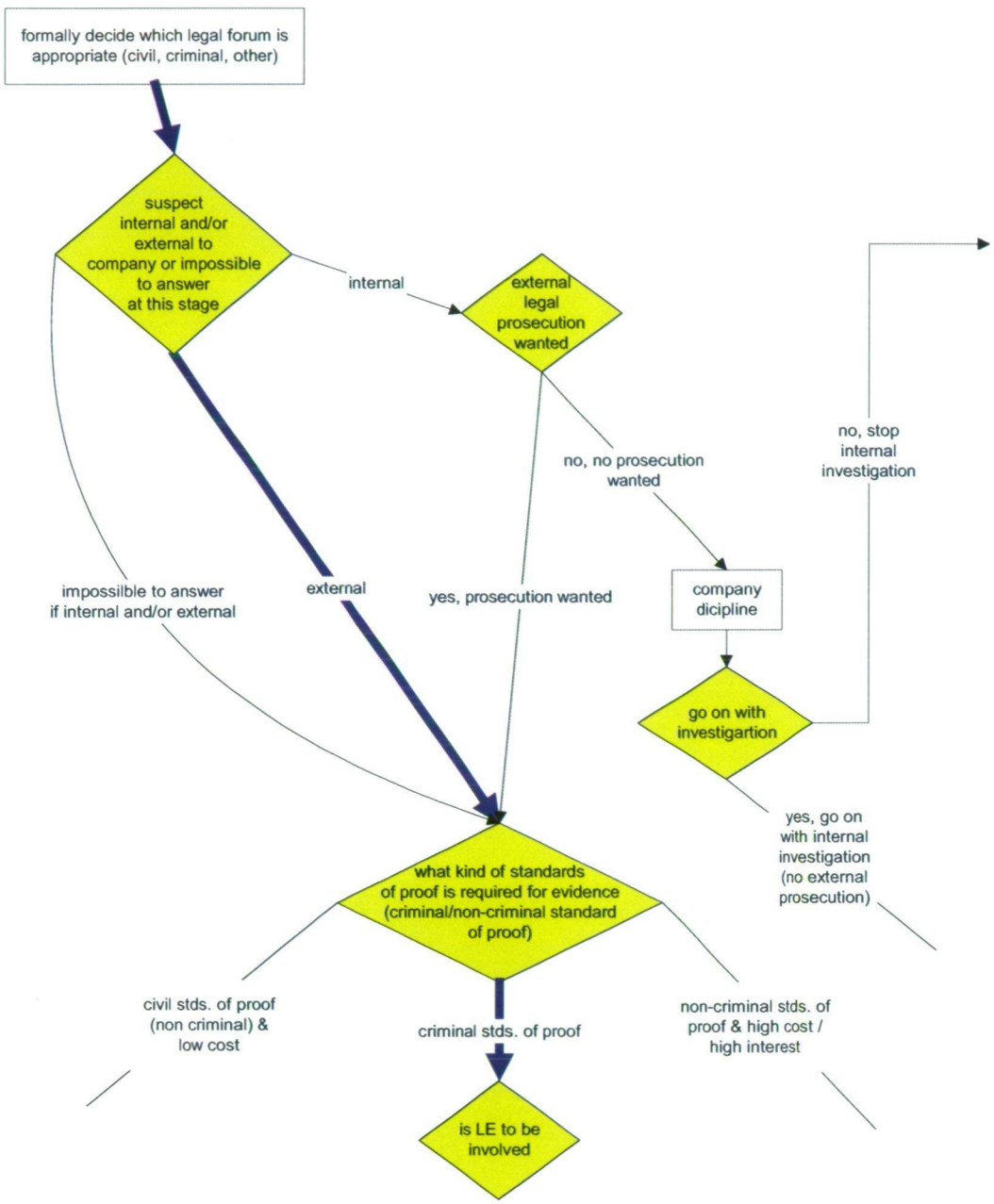


Figure 17: Fragment of the Process Model

This prototype was called the 'Cyber Crime Advisory Tool' (C*CAT) and is made up of a database connected to a database administration tool containing all actions, decisions, relationships (sequence of flow charts) and all additional information. The architecture of C*CAT is presented in Figure 18.

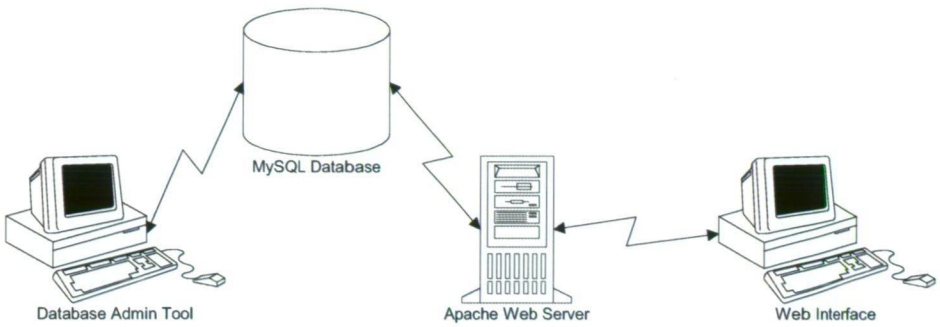


Figure 18: C*CAT Architecture

The Web based front end of C*CAT (see Figure 19 and Figure 20), connected via an Apache Web server to the database, is the interface between the information to be processed and the people involved in investigating a computer misuse incident.

Figure 19: C*CAT's Web Based Interface, part 1

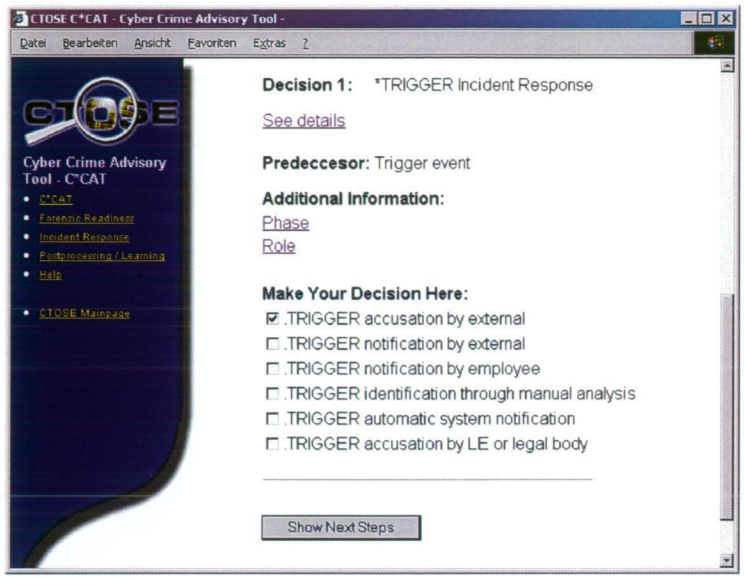


Figure 20: C*CAT's Web Based Interface, part 2

From the evaluation of C*CAT, it is clear that it is easy to use, and allows users to define the situation (by selection among different choices). Following this phase C*CAT presents the necessary actions and decisions that should be taken. In each case the user is able to ask for more advice and guidance. Since the integrity of the chain of custody is critical, following correct procedures is of vital importance. At the end of the process, the user will be able to give feedback concerning the usage of the model to further improve its operation and utility.

The future aim of CTOSE was to refine and improve the methodology and distribute it as widely as possible. As part of these activities the CTOSE project has developed a simulation environment (CTOSE Demonstrator) as an educational awareness and validation tool. The demonstrator describes the process model using several different scenarios. Each scenario provides the user with a clear and understandable way to proceed with do's and don'ts when handling digital evidence for each phase.

The project anticipated that the widespread utilisation of the CTOSE methodology would assist companies in being able to recover more rapidly from computer misuse incidents and improve their ability to conduct computer

forensic investigations (Frings, et al., 2003; Urry & Mitchison, 2003). The CTOSE project has unquestionably made a very significant contribution to the development of a methodology for a standardised approach to computer misuse. Unfortunately, the next phase of the project – commercialisation – failed completely.

6.4 Preliminary Findings for Case C

The CTOSE project produced so far most comprehensive model and methodology for forensic computing. It contributed by accepting the facts that forensic computing investigation is not limited to criminal law environment only. On the other hand it produced very complicated model that has unfortunately proved too complicated to be widely adopted, if not adopted at all.

Additionally, although the project was deemed to be highly successful, some of the involved researchers now admit, that it needs further improvement (e.g. Frings, 2006).

In working towards a more integrated solution that balances requirements for network security, individual privacy and the need for legally admissible digital evidence, CTOSE project confirmed recommendations previously articulated by Broucek & Turner (2004a):

- Best practice for digital evidence handling should involve deploying the highest investigative standards at all stages in the identification, analysis and presentation of digital data;
- Targeted training and education of network administrators and end-users in the key principles of digital evidence handling is urgently required. As is education and awareness amongst users of the consequences of their on-line behaviours for system security;
- Opportunities exist for the further refinement of e-forensic methodologies and processes such as those developed by CTOSE and these must include

recognition of the dynamic and multi-faceted nature of the forensic computing domain; and

- Enhancing e-forensic professionalism through the rapid development of processes for e-forensic computing competences and certification is an essential element in building and implementing integrated solutions.

This case confirms that organisations continue to face significant challenges in responding to threats of criminal, illegal or inappropriate on-line behaviours (see 2.2.2). Management approaches and the development of policies and procedures continue to be developed in this area as part of the solution for these challenges (see 2.6.1 and 2.6.2). However, this chapter also reveals that these developments, aimed at responding to the challenges pose their own issues for adoption, implementation and use.

6.5 Summary Reflection on the Chapter

This chapter provided analysis of the development, outputs and results of EU funded Cyber Tools On-Line Search for Evidence (CTOSE) project through analysis of the framework and a review of its achievement and results following completion of the project. As a result of the researcher's close collaboration with the CTOSE project, this analysis is able to examine some of the key issues that inhibited the framework's commercialisation, adoption and use by organisations for whom it was developed. The analysis highlights the practical challenges faced at the organisational level in the implementation of models and tools for digital evidence handling. The analysis highlights that models and tools that have been developed for handling digital evidence are by their very nature and complexity highly problematic to adopt and utilise in organisational settings. A key element that continues to inhibit their use is the lack of early and comprehensive end-user education. The results highlight amongst others the critical need for organisations to have greater 'forensic readiness' for dealing with criminal, illegal or inappropriate on-line behaviours.

7 Interpretation and Discussion: Forensic Computing Perspective[14]

"The outcome of any serious research can only be to make two questions grow where only one grew before." (Thorstein Veblen, 1857-1929)

7.1 Introduction

By adopting a forensic computing perspective this chapter will examine the inter-relationships between the challenges for digital evidence identified across the three cases and draw out their implications for emerging responses to criminal, illegal and inappropriate on-line behaviours. This examination explores the inter-relationships through nine challenges which form the basis of the four key research findings.

The chapter also presents a discussion of the four research findings that support a more coherent and holistic approach to understanding, implementing and evaluating digital evidence and responses to criminal, illegal and inappropriate

---

[14] Please note some of the material presented in this chapter has been adapted from materials first published in the following peer reviewed publications:

Broucek, V., & Turner, P. (2005). "Riding Furiously in All Directions" - Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-line Behaviours. In P. Turner & V. Broucek (Eds.), *EICAR 2005 Conference Best Paper Proceedings* (pp. 190-203). Saint Julians, Malta: EICAR.

Broucek, V., & Turner, P. (2005). Considerations for e-forensics: Insights into Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-line Behaviours. *International Scientific Journal of Computing, 4*(2), 17-25.

Broucek, V., Turner, P., & Frings, S. (2005). Music piracy, universities and the Australian Federal Court: Issues for forensic computing specialists. *Computer Law & Security Report, 21*(1), 30-37.

Broucek, V., & Turner, P. (2006). Winning the Battles, Losing the War? Rethinking Methodology for Forensic Computing Research. *Journal in Computer Virology, 2*(1), 3-12.

on-line behaviours. It is anticipated that these forensic computing findings will contribute to addressing the inherent paradoxes across technical, legal and organisational domains.

From the three cases described in previous chapters it has been confirmed that each area is facing its own significant challenges. Research and development in each area is working on solutions for these challenges, and some examples have been provided. However, this research has also highlighted that these developments tend to concentrate on 'fixing their own' challenges without consideration of any knock-on effects for other areas.

From a forensic computing perspective, this raises concerns about digital evidence and about the inter-relationships amongst technical, legal and organisational solutions being developed. More specifically, the concern is that these solutions are adversely impacting on one another with detrimental impacts for digital evidence and responses to computer misuse (see 2.2.2). Before exploring these inter-relationships across the three cases, it is useful to revisit the primary research questions.

Research Question 1: What are the key technical, legal and organisational challenges of digital evidence?

Research Question 2: What inter-relationships exist between technical, legal and organisational approaches and what implications do these have for the responses being developed?

Analyses in chapters 4, 5, and 6 have generated insights that contribute directly to answering these questions. The first part of this chapter will revisit the analyses from these chapters and adopting a forensic computing perspective will identify challenges for digital evidence.

7.2 Interpretation across three Cases

Analyses of the data from the three cases presented in chapters 4, 5 and 6 have identified challenges for digital evidence from technical, legal and

organisational perspectives. This section aims to examine the inter-relationships amongst these challenges and to interpret their significance for emerging responses to criminal, illegal or inappropriate on-line behaviours.

7.2.1 Key Inter-relationships and Digital Evidence

In examining the key inter-relationships amongst the challenges identified in each case, this section commences by drawing on the technical challenges identified in Case A and explores their inter-relationships with the other cases. This is followed by an examination of the legal challenges identified in Case B in relation to the other cases. Finally, this section explores the organisational challenges identified in Case C in relation to the other cases.

The key technical challenges identified in Case A are:

1. Quality of collected data including factors of its reliability, completeness and correctness;
2. Problems with establishing clear timelines;
3. Need for correlation of data from various sources including possibility of tainting the data during the process; and
4. Reproducibility of analysis of these data using various and even same tools.

Challenge 1: Quality of collected data including factors of its reliability, completeness and correctness.

Case A demonstrates that quality of data collected by SNORT is questionable for the purposes of computer security and intrusion detection. The data collected by SNORT may not be complete, may not be able to give a 'full picture' and most importantly can even be incorrect. This has been clearly demonstrated by the identification of a bug in the version used for the experiment. Significantly, this illustrates that from a technical perspective, the system is not providing the protection that it is ostensibly designed to provide. As it will be discussed in section 7.3, solutions being developed to respond to these technical issues further compound the challenges for digital evidence.

From a legal perspective, the fact that the data cannot be guaranteed complete or correct renders such data inadmissible or at least invalid in court of law (Sommer, 1998b). This directly supports Sommer's conclusion that

> *"current intrusion systems are not designed to collect and protect the integrity of the type of information required to conduct law enforcement investigations" (Sommer, 1998b).*

From an organisational perspective, the unreliability of the data potentially creates an increased workload on system personnel who need to analyse the data. It also puts organisation in the risk of false alarms and/or can make organisation falsely believe that it is protected against intrusion detection while it may not actually be protected at all. Alternatively, the organisation may wrongly accuse another organisation for wrongdoing as it could easily happen in the Case A study.

Challenge 2: Problems with establishing clear timelines

The case study demonstrates that various computer security tools needed to analyse collected data can produce different time stamp results. While this may not be relevant for IDS purposes, this might be a significant factor if such data were to be used as digital evidence.

From a legal perspective this challenge creates a similar legal challenge as the Challenge 1 above. This could additionally cause issues regarding chain of evidence rules and correct timeline.

From an organisational perspective this might not be such a big problem, until the organisation decides that it wants to use the data as digital evidence. Yet again, this shows how closely all the areas are inter-related.

Challenge 3: Need for correlation of data from various sources including possibility of tainting the data during the process

Data collected by the tool itself may not be enough to produce enough data to ascertain real source of intrusion. There is a need to correlate data from

different sources to get 'full picture'. Such correlation can be done either by hand or by another computer tool. Both approaches further problematicise quality of final data as they both can create errors or misinterpretation. It has indeed been shown that at least one commercial product actually misinterpreted data collected in Case A so much that it has been dropped from this thesis.

From a legal perspective, the need for correlation of data from various sources poses significant challenge. The correlated data are different from 'original data' and questions of chain of the evidence are immediately raised. The manipulation of original data can again create errors. Additionally, questions of reproducibility would arise from such manipulation again. For correlation of data from various sources, common attribute is needed. This attribute is obviously the time; however, it has been shown in Challenge 2 above that technical tools have problem with keeping correct time stamps.

From an organisational perspective, this brings expense and need for additional resources both in technical area as well as in human resources. Correlation of digital data where gigabytes of it are collected is nearly impossible to do 'by hand' and suitable tools can be very expensive, complicated to use and they often require significant computing resources.

Challenge 4: Reproducibility of analysis of these data using various and even same tools (different versions producing different results)

The case study demonstrated that reproducibility of the results is questionable. Various tools will produce different results (for example different resolution of time stamps from exactly same data) and even re-analysing the collected data with newer version of the same tool can produce different result. This has been confirmed when the data was re-analysed with version that fixed bug identified in the cases study.

From a legal perspective, this challenge only reinforces legal implications of Challenges 1 – 3 above. As various forensic experts have access to different tools, this reinforces calls for standardised testing and evaluation of forensic

tools. It has been shown in Case B that University of Tasmania did not have access to EnCASE tool used by the counsel for music industry and this caused significant questions about the process of e-discovery in the case. The case being about breach of copyright, it was rather interesting when forensic expert for music industry offered the University of Tasmania to loan his license to run EnCASE locally ("Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003)," 2003). It is author's opinion that this would be in direct breach of EnCASE licensing agreement.

From an organisational perspective, this highlights need for the organisations to be ready for possible investigation. This yet again reinforces calls for 'forensic readiness' to be part of organisational standard ICT policies and procedures.

Compared with the speed of development in the technical area, development in legal area is often very slow and cumbersome. Development of new laws is often very slow and complicated by the need to satisfy many other requirements than just legal. Political issues can play significant role as it has been apparent in post 9/11 developments in anti-terrorism laws.

The key legal challenges identified in Case B are:

5. Legal validity and admissibility of collected data;
6. Questions of privacy and confidentiality; and
7. Lack of technical knowledge by legal profession.

Challenge 5: Legal validity and admissibility of collected data

The problem of legal validity and admissibility of evidence (collected data) is well understood by legal profession but not by people who actually collect the data. It has been shown that legal validity and admissibility evidence used in Case B was at least questionable. No proper forensic technique was used to collect initial evidence and subsequent copying of initial backups from tapes to the set of hard disks for further analysis by forensic expert was done by one of

the system administrators at the University premises without proper control of the chain of the evidence.

From a technical perspective this again stresses the fact that current computer security or standard system utilities (for example backup utilities as used in the case of the University of Tasmania) were not designed to collect digital evidence.

From an organisational perspective, the case supports the notion of forensic preparedness for companies. If a company is approached to collect data by outside request or if the need arises internally, the company has to be prepared to do so in forensically sound way – that is in a way that will produce data (or evidence) suitable as an evidence in a case of criminal, illegal or other inappropriate on-line behaviours. It has been recommended (e.g. CTOSE project) that organisation always attempts to collect data in the highest possible quality; that is as if it were preparing for criminal case.

This requirement of course means that company needs to have not only suitable tools, but also suitably trained personnel. Additionally, it has to have in place policies and procedures to manage this.

Challenge 6: Questions of privacy and confidentiality

The Case B demonstrates that improperly conducted collection of digital evidence and/or even discovery of such evidence can have significant implications for privacy and confidentiality. In the case analysed in Chapter 5, the request was made for copy of e-mails of all members of the University of Tasmania (all students and staff). This could have significant implication for confidentiality of student data and more significantly for the confidentiality of research being conducted at the University. It has been commented by McCullagh and Caelli (2003) (Professor Caelli being one of the leading computer security experts) that

> *"A further point about this case is that the court has in effect condoned an organisation, in this case Sony, to undertake a fishing expedition for*

evidence in the possession, power or control of a third party. It is similar to an order that party A (Sony) has the right to rifle through a filing cabinet or filing cabinets under the possession power or control of party B (the Universities) so as to locate some information (the certainty of which is unknown) that may incriminate party C who at the time is indeterminate (unknown university students)."(McCullagh & Caelli, 2003)

From a technical perspective, this challenge again raises the question of 'how much data to collect'. As it has been shown, probably most ideal situation would be to collect 'everything'. Unfortunately, such solution is technically impossible and collecting 'everything' is usually viable for short time purposes only. Even if it was possible, then the issues of privacy arise again and techniques would have to be developed to protect individuals' privacy. At the same moment, the same techniques would have to enable efficient investigation and analysis of collected data. These two requirements of course are contradictory and demonstrate one of the biggest paradoxes of today's world of computer security and forensic computing.

From an organisational perspective, this challenge highlights how lack of pro-active measures can cause risk to organisation's intellectual property, its employees' privacy and possibly to confidentiality of data being held on organisation's digital systems. While the University of Tasmania had appropriate policies about usage of University networks and computers in place, there were no procedures in place to avoid this legal case.

Challenge 7: Lack of technical knowledge by legal profession

Legal profession lacks in the knowledge of contemporary technology, judges are often nearly computer illiterate. Judges have poor understanding of technological terms. The case demonstrates this fact on judge's insistence of producing backup tapes that have already been overwritten with different data as a source of possible evidence.

From a technical perspective, this means that developers of technical solutions for digital evidence must keep in mind that they are not dealing with computer professionals but rather with audience with limited computer knowledge. In some legal systems this does not mean judges only, but also juries. The tools and techniques being developed seem to be concentrating more on computer professionals and while some of the presentation capabilities of these tools are impressive, to understand these is sometimes difficult even for computer professionals (for example 3D visualisation graphs used in tool called CA eTrust Network Forensics).

From an organisational perspective, this means that organisation must be prepared to deal with sometimes unreasonable requests and be prepared to produce materials suitable for personnel without much technical knowledge. It is even more important to realise that digital evidence must be understandable by personnel with limited technical knowledge in cases of inappropriate on-line behaviours that are not being dealt with by courts, but for example by internal investigation only.

The key organisational challenges identified in Case C are:

8. Lack of user education; and
9. Problematic or missing policies and procedures.

Challenge 8: Lack of user education

The case study demonstrated that lack of user education at end-user, network administrator and management levels can lead organisations to face numerous challenges in detecting, reporting, managing and responding to computer misuse. For example, a lack of end-user education about proper use of e-mail illustrates the potential for computer security and privacy issues to arise by the use of inherently insecure products (for example POP based e-mail systems) (Broucek & Turner, 2002b). Despite technical awareness of the insecure nature of the POP protocol (Myers & Rose, 1996), it is still widely used by many organisations who would profess to be concerned about computer misuse.

From a technical perspective, lack of user education may lead towards incorrect use of tools not suitable for specific tasks. This user education must be understood as education of end-users as well as systems administrators and most importantly the management. As an example, individuals concerned about their privacy and security may adopt encryption tools to increase their sense of security and privacy. Unfortunately, while this can increase the technical security of the data, it is easy for end-users to implement it incorrectly or to manage their encryption keys insecurely, thereby undermining the encryption protocols. For organisations, these end-user behaviours can also pose significant problems, including data access and management, commercial confidentiality and employee management.

From a legal perspective, the use of encryption by individuals as well as by public and private sector organisations has become increasingly common. For policy-makers access to encryption creates issues in relation to law enforcement, privacy and surveillance powers. Clearly for criminals, hackers and other individuals engaging in illegal or inappropriate behaviours, encryption provides protection. As the Aldrich Ames Spy case illustrated (Reno, 1996), encrypted data files obtained as part of an investigation are basically useless as evidence.

Challenge 9: Problematic or missing policies and procedures

The case study also confirmed that problematic policies, policies that are not explained and/or are too draconian can cause more trouble than benefit. As it has been noted, imposing unnecessary restrictions on use of company e-mail accounts for private purposes may lead to wide spread adoption of unauthorised software, for example access to 'free' e-mail services (Gmail, hotmail, yahoo etc) (Broucek & Turner, 2002b). Ultimately this ends up increasing the security risks faced by organisations, as the typical end-users may be 'lazy' or complacent about the use and re-use of usernames and passwords.

From a technical perspective, problematic policies dramatically increase the burden of 'unnecessary' monitoring, perceptions of 'big brother' surveillance and may lead to creating an environment of fear and self-monitoring that may produce further unhelpful behaviours in the organisation.

From a legal perspective, both employees and organisations are increasing the risk of breaches of personal privacy, but also significantly the risk of increased vulnerability to loss of intellectual property and other criminal, illegal or inappropriate on-line behaviours.

This section has presented an exploration of the inter-relationships amongst technical, legal and organisational challenges identified in Chapters 4, 5 and 6. This exploration has highlighted the inter-connectedness across these domains.

The next section of this chapter presents a discussion of the research findings and considers them within the context of the research literature (see Chapter 2). The four key research findings are based on a synthesis of the nine challenges examined above.

7.3 Discussion of Findings

The section presents a discussion of the research findings that support a more coherent and holistic approach to understanding, implementing and evaluating digital evidence and responses to criminal, illegal and inappropriate on-line behaviours. It is anticipated that these forensic computing findings will contribute to addressing the inherent paradoxes across technical, legal and organisational domains.

From the definition of forensic computing advocated by Broucek & Turner (2006) as being

> *"processes or procedures involving monitoring, collection, analysis and presentation of digital evidence as part of 'a priori' and/or 'post-mortem' investigations of criminal, illegal or other inappropriate on-line behaviours"*

and the taxonomy of forensic computing developed by Broucek & Turner (2001a, 2001b) and further expanded by Hannan, Frings et al. (2003) and Hannan, Turner et al.(2003), it is clear that technical, legal and organisational responses to computer misuse are intimately related and influence each other.

The taxonomy covers a broad range of issues and approaches impinging on the emerging discipline of forensic computing. It highlights that any coherent research framework must acknowledge differences in the focus of the approaches: individual, organisational, national, and supra-national; differences in the scale of systems: personal computer and other individual devices; intranet; extranet, VPN and the Internet; and differences in the participants and audiences engaged in these topics.

The key findings from this research thesis are:

1. Data collected by computer security tools can contain errors, be incomplete or be open to incorrect analysis and interpretation. Collected digital data alone, rarely provide enough data to confidently generate a complete picture of what has happened on the system and how this relates to any computer misuse and the 'last mile' connection with identifiable user.
2. Current approaches towards 'forensic readiness' within technical, legal and organisational domains continue to be merely a 'band aid' approach that appears to be increasingly ineffective. Presuming forensic capacity or trying to add it post facto is unlikely to be effective going forward. It is therefore necessary to start developing technical tools, legal frameworks and organisational policies that contain 'forensic readiness' in their designs.
3. Lack of education and training about the inter-relationships between technical, legal and organisational responses to computer misuse is inhibiting the development of coherent and holistic approaches to forensic computing. Critically, for organisations (public and private) this requires a more proactive approach to acknowledging these inter-

relationships in their approaches to detecting, reporting and managing criminal, illegal or inappropriate on-line behaviours.

4. Current approaches to 'technology neutral' legislation are sensible, but they need to be more coherently embedded in 'technology neutral' legislative frameworks that can operate within and between jurisdictions (local, national, international). At the level of legal practice there is a need for widely agreed 'best practices' for collection, preservation and presentation of digital evidence and standardised testing and evaluation of the tools and for certification of expert witnesses.

Next section discusses each finding in more detail.

Key Finding 1: Data collected by computer security tools can contain errors, be incomplete or be open to incorrect analysis and interpretation. Collected digital data alone, rarely provide enough data to confidently generate a complete picture of what has happened on the system and how this relates to any computer misuse and the 'last mile' connection with identifiable user.

It is not possible to rely on existing technology to provide fully reliable evidence. It has been validated in this research that some tools used for collection of electronic evidence can provide both erroneous as well as incomplete data. In many cases, even where evidence is correlated from several different tools to obtain an improved analysis and interpretation of the data, challenges remain. This correlation can be done manually, potentially introducing human error factor, or using other tools, introducing again both human factor (tool used incorrectly) and/or problematic functionality of the new tool.

Case A clearly demonstrates that the results obtained were at least misleading, if not completely erroneous. It also clearly demonstrates that data obtained from the tool were not good enough to identify the misleading information, and that additional data or further investigation was needed. These points clearly demonstrate how current gaps in technology can be used by attackers

deploying anti-forensic tools. For example, to avoid detection attackers can use the 'decoy' mode of the NMAP tool that is used for network reconnaissance and probing to avoid detection (see 2.4.4).

Additionally, it is important to realise, that digital data alone cannot identify the actual user of the digital device. This can particularly be a problem in shared environments (computer labs) and be compounded by bad user practices (sharing passwords, leaving computers while being fully logged in etc). This fact calls for recognition of 'last mile' problem (Hannan & Turner, 2004). This problem highlights that the person involved in conducting criminal, illegal or inappropriate behaviour may not be the person whose login credentials are currently used at the computer. For forensic computing investigators it also highlights that they need to address the possibility of the computer being compromised and used as an intermediary in their investigations otherwise they are open to the legitimate legal defence of SODDI type (see 2.5.3).

Key Finding 2: Current approaches towards 'forensic readiness' within technical, legal and organisational domains continue to be merely a 'band aid' approach that appears to be increasingly ineffective. Presuming forensic capacity or trying to add it post facto is unlikely to be effective going forward. It is therefore necessary to start developing technical tools, legal frameworks and organisational policies that contain 'forensic readiness' in their designs.

With the exception of several products developed specifically for forensic analysis of electronic evidence, most of computer security tools that 'could' provide forensic evidence do not provide it. Furthermore, the development in computer security tools makes this even more complicated, since the presumed increased security is often making it impossible or more difficult to collect any forensically sound data. One example could be development of Intrusion Prevention Systems (IPS) instead of Intrusion Detection Systems (IDS). While the later was only detecting and alerting with the possibility of collecting some (albeit questionable data), the new system simply 'pulls the plug' on possible attacker without giving any evidential data.

Both Key Finding 1 and Finding 2 are well support by the body of available literature and by findings by other researchers as discusses in 2.4.2 and 2.4.3.

Resulting from these two findings are two paradoxes of current understanding of the play, where:

1. Increased sophistication of technical measures hampers capability of these measures to collected digital evidence; and
2. There still exist the misconception that forensic computing is equal or at least is part of computer security (see 2.4.1).

Key Finding 3: Lack of education and training about the inter-relationships between technical, legal and organisational responses to computer misuse is inhibiting the development of coherent and holistic approaches to forensic computing. Critically, for organisations (public and private) this requires a more proactive approach to acknowledging these inter-relationships in their approaches to detecting, reporting and managing criminal, illegal or inappropriate on-line behaviours.

Many organisations do have security policies, usage agreements and risk management policies, but there is visible lack of forensic policies. This in turn creates lack of preparedness. Organisations are prepared to deal with breach of security by plugging security holes, installing patches, but there are hardly policies/procedures for proper investigation – again, business continuity has highest priority mostly.

Organisations are still unprepared. This was demonstrated by:

- Development of CTOSE and inability to commercialise this project although the results were considered to be very good and promising (Case C); and
- The way collection of the evidence was handled in the RI v. AU (Case B).

Users are uneducated and often threatened by security and privacy policies imposed on them by organisations. In many cases they do not receive proper

explanation of why and what for these policies are. Cases have been reported where end user that was sure of not doing anything wrong rather paid ransom money than calling security officer in fear of being dismissed from the company.

Many organisations spend vast amount of money on training system and network administrators, on computer security tools, on establishing computer security officer positions, but rarely do they spend much on forensic readiness. In many cases, collection of evidential material is done by system and network administrators without minimal or even no knowledge of proper collection of the evidence, not mentioning proper handling of it and its continuity.

It has been noted in Challenge 9 above, that imposing unnecessary restrictions on use of company e-mail accounts for private purposes may lead to wide spread adoption of unauthorised software, for example access to 'free' e-mail services (Gmail, hotmail, yahoo etc) (Broucek & Turner, 2002b). Ultimately this ends up increasing the security risks faced by organisations, as the typical end-users may be 'lazy' or complacent about the use and re-use of usernames and passwords.

This leads to situation where it can be concluded that:

- User education does not work, or
- Temptation of the technology is bigger than the fear and desire for privacy, or
- Perhaps computer security people are too much concerned.

Something needs to be done and it clearly demonstrates need for:

- Change and improvement in education of managers and decision makers in the organisation since the current situation is often cause by:
    - lack of money,
    - inertia in the system that is in paradox with rapid change in technology,
    - wrong pretence of better security,

- wrong understanding of the need for monitoring and data collection (e.g. collection of proxy log files as possible evidence of visited sites by individual users for cases of inappropriate usage – these log files do not have any value, since they only show 'who authenticated' during the access, but not who was sitting in front of the computer – 'last mile problem'),

- Change and improvement in education of systems administrators who often blindly follow management orders or have to work with whatever they have available and provide substandard, insecure and privacy breaching products to the users.

Business continuity is often more important than investigation and instead of allowing continuous investigation of the security breach, company rather 'pulls the plug'. From the perspective of allowing ongoing security breaches for evidence acquisition, it is clear that the Rome Labs case (Christy, 1998), the Mitnick case (Shimomura, 1995), the development and use of 'Honey pots' (Even, 2000; Spitzner & Roesch, 2001a, 2001b) and the tracking of computer espionage (Clifford Stoll, 1988; Cliff Stoll, 1989) provide strong arguments against 'pulling the plug'. These cases illustrate the advantages for forensic investigations of tracking and tracing hackers during ongoing security breaches. On the flipside of this, the highly published Microsoft case (B. Bace, 2000; Leyden, 2000; Maher, 2001; Microsoft Responds to Security Issue," 2000; Mitnick, 2000; Poulsen, 2000; Rohde, 2000; Sliwa, 2000; Verton, 2000; Weiss & Rosencrance, 2000) highlights how sensitive this issue can be, particularly for information and communication based industries. Here business reputation as well as specific commercial data are at risk and must therefore be protected.

Key Finding 4: Current approaches to 'technology neutral' legislation are sensible, but they need to be more coherently embedded in 'technology neutral' legislative frameworks that can operate within and between jurisdictions (local, national, international). At the level of legal practice there is a need for widely agreed 'best practices' for collection, preservation and presentation of digital

evidence and standardised testing and evaluation of the tools and for certification of expert witnesses.

The computer crime is often multi-jurisdictional. While the actual crime (or breach of computer security later resulting in crime) can occur in one country, the perpetrator can be located in another country. It is not only problem between countries; it can also be within one country that has different state laws covering such crimes. For example, in Australia, it is often unclear whether the activity is covered by state or federal law at the beginning of the investigation.

Additionally, different countries are using different legal systems, making digital crime even more complicated. The way courts deal with new crimes is completely different in procedural legal system than in precedential legal system. The need for juries in some legal systems even increases need for having sound laws and, significantly, procedures for presentation of digital evidence. In these systems the lack in knowledge of modern technology by judges, barristers and other legal professions is compounded by need to deal with jury. Members of jury can have even less knowledge, or significantly better knowledge, particularly in younger generation.

An example of a judge's poor understanding of technology has been given in Case B where the judge's ruling was that overwritten magnetic tape is in his learned opinion equal to deleted magnetic tape. Lawyers are also often lacking technical knowledge, although the 'new generation' are starting to appear and developing expertise in niche fields such as intellectual property and electronic crimes. Consequently, this 'poor understanding' by judges could possibly be exploited by knowledgeable defence lawyers using novel and unusual tactics, for example 'Trojan horse type defence' or 'addiction to hacking' type defence as discussed before (see 2.5.3).

The need for best practices has been highlighted both in Case B and Case C as well as in the available body of literature, for example (Brungs & Jamieson, 2005; Yasinsac, et al., 2003). The problems with different interpretation of

laws and best practices have been demonstrated in section 2.5.2 on example of state of Queensland requirement to use the original data (computer) during presentation in the court.

Legislation remains lacking behind developments in technology and unless technologically neutral legislation is developed, it will remain so.

Qualification requirements for expert witnesses are questionable, in some jurisdictions nearly non-existent. Access to quality equipment and forensic investigation tools is hampered by high cost and in some case by only limited availability. Interestingly, some tools are available to law enforcement agencies only. This prevents these tools from being independently examined and validated. This in turn creates difficulties in validating the evidence. In some cases (RI v. AU) prosecution has access to the tools; however, the tools are not available to the defence.

At the broadest level, these four key research findings reveal the complex inter-relationships in the forensic computing domain and confirm that they are likely to continue into the future as a result of uncoordinated research and development, commercial product development and difficulties of legal theory and practice.

The underlying paradoxes prevalent within the forensic computing domain result from the different concerns, interests and expectations of stakeholders and the nature and foci of research and development in each domain. This in turn ultimately leads to developments that are beneficial for improved performance in one area and at the same moment creates new challenges and inhibitors in another area. These circumstances have the on-going potential to trigger 'chain reactions' that ultimately may lead to more significant challenges than the problems they solve.

This research also reveals that the digital domain itself is also intimately related to the physical world where corroborative evidence and conventional investigative techniques have an equally important role to play. Ultimately, it is

human behaviours that create these ongoing opportunities, challenges and risks. As a result, 'forensic readiness' also implies being able to grapple with moral, ethical and even political dimensions of these debates across the 'last mile' connection between digital behaviours and identifiable citizens.

In this context, forensic computing emerges as an approach that does not advocate for stronger laws, stricter technical systems and/or organisational protocols per se, but rather for the beginning of dialogue amongst these different requirements. In responding to the complex inter-relationships and definitional problems identified in this research, it is clear that solutions developed need to be aware of their specific aims and objectives as well as the broader context, if we are to avoid the on-going 'band-aid' approaches.

7.4 Summary Reflection on the Chapter

This chapter provided an interpretation and discussion of the complete data set. The interpretation of the data brought together analyses conducted in Chapters 4 to 6.

The interpretation and discussion of the analyses from the three cases adopted a forensic computing perspective and focused on the nature of the inter-relationships between the issues identified in each case. From this perspective the discrete approaches adopted in each case limit an appreciation of the complex interplay between technical, legal and organisational factors. This interplay continues to have serious implications for each of these areas because of the nature of digital environments. More specifically this interpretation and discussion reveals how and why this continued fragmentation of discrete approaches is impairing the overall effectiveness of the responses developed. A consequence of this is the lack of integrated and coordinated solutions that would effectively balance requirements for legally admissible digital evidence, effective e-security and data privacy.

8 Conclusion and Future Work

"If we knew what it was we were doing, it would not be called research, would it?" (Albert Einstein)

8.1 Introduction

This thesis concludes by providing a brief synthesis of the major challenges identified and the key research findings. This chapter discusses the contributions this thesis makes to the development of forensic computing and to understanding of complex inter-relationships between three major areas – technical, legal and organisational.

This thesis addresses two research questions:

Research Question 1: What are the key technical, legal and organisational challenges of digital evidence?

Research Question 2: What inter-relationships exist between technical, legal and organisational approaches and what implications do these have for the responses being developed?

8.2 Synthesis of Findings

This section presents a short summary review of this research. The first three parts briefly summarise preliminary conclusions generated from chapters 4, 5 and 6.

8.2.1 Technical Area

Case A (see Chapter 4) has presented a case study on use of SNORT intrusion detection system as a possible candidate for collecting digital evidence data. The case study demonstrated that the technology faced significant problems of its own. The case study revealed these problems and documented them on an example of data collected at the University of Tasmania.

The analysis of the Case A concluded (see 4.5) that:

- IDS systems may collect only a partial data set – it has been shown that data collected by SNORT were not sufficient to track and trace attackers and that the data collected in the case of encrypted communication using SSL had no value in this regard; and
- The data sets collected may be flawed, erroneous or already have been tampered with – it has been shown that even with significant fine-tuning SNORT produced numerous false positive alerts and/or wrongly identified the source of attacks.

More significantly, the case study has highlighted that from a legal perspective IDS, the data they produce and how that data is analysed, pose numerous challenges for those interested in evidence acquisition that produces legally admissible evidence. In particular, even where data has been captured the process of its technical analysis may invalidate it in terms of legal admissibility by 'tampering' with the evidence.

The case study has also highlighted that the 'collect everything' approach is highly desirable but has severe limitations and implications.

The study also confirms that Intrusion Detection Systems can play an important role in protecting Information Systems infrastructure. However, to be effective they require attention of highly trained security personnel/system administrators.

8.2.2 Legal Area

Case B (see Chapter 5) presented analysis of one particular legal case in the Federal Court of Australia.

It has been revealed that even where digital evidence is available and has been accepted as admissible, critical issues have emerged over the understanding of the courts on the nature of this evidence. For example, this particular case being a dispute over the distribution of MP3s by students and staff at the

Universities reveals a "*worrying lack of comprehension of the technical nature of digital logs and data storage*" (Broucek, et al., 2003; Broucek & Turner, 2004a; Broucek, et al., 2005). More specifically, this lack of understanding resulted in the provision of access to data sets that contained information on the on-line activities of thousands of presumably innocent users and not just data on those alleged to be guilty of computer misuse. This provision of unprecedented access to huge amounts of potentially sensitive data pertaining to the personal, confidential and commercial activities of innocent users is clearly of concern and has been called by some authors "*fishing expedition*" (McCullagh & Caelli, 2003). This is especially the case where access to the data was not handed over to an independent third party.

8.2.3 Organisational Area

Case C (see Chapter 6) presented an analysis of the Cyber Tools On-Line Search for Evidence (CTOSE) project.

It can be concluded that the CTOSE project produced so far most comprehensive model and methodology for forensic computing. It contributed by accepting the facts that forensic computing investigation is not limited to criminal law environment only.

On the other hand, it produced very complicated model that has unfortunately proved too complicated to be widely adopted, if not adopted at all. This concern has been confirmed by failure of this project to commercialise and as far as the author is aware only one organisation in Europe is still using the CTOSE methodology.

The next part below summarises the interpretation of the inter-relationships from Chapter 7.

8.2.4 Forensic Computing Perspective

Each case study revealed its own set of challenges, the inter-relationships amongst these cases were presented in chapter 7 (see 7.2.1). A total of nine challenges were presented:

1. Quality of collected data including factors of its reliability, completeness and correctness;
2. Problems with establishing clear timelines;
3. Need for correlation of data from various sources including possibility of tainting the data during the process;
4. Reproducibility of analysis of these data using various and even same tools;
5. Legal validity and admissibility of collected data;
6. Questions of privacy and confidentiality;
7. Lack of technical knowledge by legal profession;
8. Lack of user education; and
9. Problematic or missing policies and procedures.

The next part of this section briefly summarises the key research findings first presented in chapter 7 (see 7.3). These four key research findings are based on a synthesis of the nine challenges outlined above.

The key findings from this research thesis are:

1. Data collected by computer security tools can contain errors, be incomplete or be open to incorrect analysis and interpretation. Collected digital data alone, rarely provides enough data to confidently generate a complete picture of what has happened on the system and how this relates to any computer misuse and the 'last mile' connection with identifiable user.
2. Current approaches towards 'forensic readiness' within technical, legal and organisational domains continue to be merely a 'band aid' approach that appears to be increasingly ineffective. Presuming forensic capacity

or trying to add it post facto is unlikely to be effective going forward. It is therefore necessary to start developing technical tools, legal frameworks and organisational policies that contain 'forensic readiness' in their designs.

3. Lack of education and training about the inter-relationships between technical, legal and organisational responses to computer misuse is inhibiting the development of coherent and holistic approaches to forensic computing. Critically, for organisations (public and private) this requires a more proactive approach to acknowledging these inter-relationships in their approaches to detecting, reporting and managing criminal, illegal or inappropriate on-line behaviours.
4. Current approaches to 'technology neutral' legislation are sensible, but they need to be more coherently embedded in 'technology neutral' legislative frameworks that can operate within and between jurisdictions (local, national, international). At the level of legal practice there is a need for widely agreed 'best practices' for collection, preservation and presentation of digital evidence and standardised testing and evaluation of the tools and for certification of expert witnesses.

8.2.5 Conclusion

This research thesis concludes that there is no easy solution to resolve the inter-relationships and paradoxes inherent within forensic computing issues. However, by recognising that these paradoxes exist, how they work and what their impacts are, measures can be developed to reduce their negative effects.

This research proposes that only coordinated academic research contributing to the emergence of cohesive and holistic approaches to understanding, implementing and evaluating the paradoxes within forensic computing can produce new approach to forensic computing.

Without a cohesive and holistic approach, forensic computing will continue to suffer from uncoordinated research in all contributing areas and developments

in one area will continue compounding problems in other areas. It is anticipated that this research thesis has contributed insights that will enable a more coherent approach and mitigate the dangers of "*Riding Furiously in All Directions*" (Broucek & Turner, 2005b) and/or continuing "*Winning the Battles, Losing the War?*" (Broucek & Turner, 2006)

8.3 Limitations of the study

> *"The trouble with research is that it tells you what people were thinking about yesterday, not tomorrow. It's like driving a car using a rear-view mirror." (Bernard Loomis)*

The thesis examined only a limited part of proposed taxonomy of forensic computing, that is technical, legal and organisational area. It is envisaged that this research provides foundation to subsequent forensic computing research in the future.

The data for the three cases studies have been collected in early stages of this research. It has been conducted as part-time PhD study and subsequently some of the tools and sites mentioned in the study have been deprecated since then. At the beginning of this study in 2001, there was a very limited body of literature pertaining to forensic computing. Since 2001, the amount of available literature grew exponentially, conferences and workshops were held and several forensic computing journals appeared. This demonstrates huge interest in the topic and it can be expected that this interest will grow even more.

Case A examined one particular intrusion detection system available at the time when the data were collected. The case in no way attempts to compare SNORT intrusion detection system with another IDS and it does not attempt to determine the technical quality of the system. The main concern of this thesis was the suitability of such system for collection of digital evidence and to illustrate problems that technology faces on its own and then to illuminate problems arising from using this technology for collecting digital evidence.

Case B examined one particular legal case in context of Australian legal system. The case has been examined on a basis of available court materials (judgements and transcripts) and with additional insights gained through direct access to some of the people directly involved in the case. In the end, the case was settled out of court and the settlement conditions remain confidential.

Case C examined EU funded CTOSE project. This project received significant funding and attention across Europe and many major institutions were involved in the project. The results were considered to be very positive and it was expected that the CTOSE solutions would become 'de-facto' standard across the Europe. The analysis of the project was to some degree limited by confidentiality of some information available through direct participation in some CTOSE activities.

All research methods have a set of strengths and weaknesses. Some limitations of this research are directly linked to the selected methodology. Case study research can be influenced by the way the data collection and analysis were conducted (Galliers, 1992). Researcher's background and experiences can also affect researcher's interpretation of the data (Yin, 1994).

Further limitations of a case study research stem from the scope of the research, in particular if it is conducted as a requirement for fulfilment of doctoral thesis. The amount of time, funding and resources is strictly limited. Fortunately, these limitations are predetermined and defined by the rules and guidelines set by the University overseeing this study.

The lack of generalisability and possible research bias are possibly the biggest limitations of this study. The bias is unavoidable in any case study research. The influence of the researcher conducting the research creates a bias when data collection is in progress. In this particular case, researcher's employment as Information and Communication Technology Manager at the University and his extensive 'hands-on' experience in systems management and security could potentially create bias towards technological issues and challenges.

However, the author believes that he was as objective and unbiased as possible and the presented results can be used in general context.

8.4 Future Work

This research clearly identifies the need for targeted research into forensic computing and different prime focus in relation to which type of organisation this research is done in. It is necessary to realise that by the nature of the business they conduct, different stakeholders have completely different interest and expectations from forensic computing.

Forensic computing is a multidisciplinary field and it is imperative to follow findings and results of all the contributing fields. As it has been highlighted by recent appearance of conferences and workshops, it is necessary to conduct more research not only into human behaviour and security, but also into human behaviour and forensic computing.

Key Proposal: Existing models are not general enough to address the multi-dimensional aspects of forensic computing and the definitional ambiguities that continue to hamper the dialogue necessary to move forward. One possible solution would be to adopt a mathematical approach towards the development of a mathematical model as suggested by Filiol (2006b).

It is also necessary to address 'post 9/11 issues'. Although the 9/11 events clearly illustrated that communication networks can be heavily hit and even disabled without actually targeting them, most of the reactions appear to be of 'knee-jerk' type of reactions. New York Stock Exchange (NYSE) had to be shut down not because it would be targeted, but because it lost network connection to the rest of the world. It did not lost the network connection because the network itself would be targeted, but because there was a much longer loss of power to the area that housed major networking infrastructure and nobody anticipated that the power will be lost for so long. Emergency batteries and generators took over temporarily and then they stopped. Mobile phone networks in New York were virtually shut down not because there

would be attack on them, they simply were overloaded first and then the system could not handle it any more.

Key Proposal: Systems and procedures must be designed with maximum optimisation, with necessary redundancy and no slack in the system. Otherwise they cannot cope with an emergency.

In this context, forensic computing emerges as an approach that does not advocate for stronger laws, stricter technical systems and/or organisational protocols per se, but rather for the beginning of dialogue amongst these different requirements. In responding to the complex inter-relationships identified in this research, it is clear that solutions developed need to be aware of their specific aims and objectives as well as the broader context if we are to avoid the on-going 'band-aid' approaches.

Key Proposal: The need for rigorous testing and evaluation of software used in forensic computing.

It is clear that without rigorous testing and evaluation, software used in forensic computing will always face problems. There is a clear need for development of unified methodology for this testing and evaluation, perhaps activity similar to that of EICAR (see http://www.eicar.org/) twenty years ago is needed. Indeed, it has been mentioned during interview with Johan ten Houten, (2007b) after presentation of his paper (ten Houten, 2007a) at Digital Forensic Forum, Prague 2007, that something similar to EICAR's sample/test virus would be useful for forensic computing.

Bibliography

Allinson, C. (2002). Audit Trails in Evidence - A Queensland Case Study. *Journal of Information, Law and Technology, 2002*(1).

. Apache HTTP Server (Version 1.3.26). (2002). Retrieved from http://httpd.apache.org/

Arona, A., Bruschi, D., & Rosti, E. (1999). Adding availability to log services of untrusted machines *15th Annual Computer Security Applications Conference (ACSAC'99)* (pp. 199-206). Phoenix, AZ, USA: IEEE Comput. Soc, Los Alamitos, CA, USA.

. Aust unis in court over file-swapping. (2003). Retrieved February 18, 2003, from http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20272193,00.htm

Australasian Centre For Policing Research (2001). *Electronic Crime Strategy of the Police Commissioners' Conference, Electronic Crime Steering Committee, 2001 - 2003*: Australasian Centre For Policing Research.

Australian Bureau of Statistics. (2008). 4102.0 - Australian Social Trends, 2008 - Internet Access at Home. Retrieved November 11, 2008, from http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Chapter10002008

Australian Computer Emergency Response Team. (2001a, 8 October 2001). UNIX Security Checklist v2.0. Retrieved November 19, 2001, from http://www.auscert.org.au/Information/Auscert_info/Papers/usc20.html

Australian Computer Emergency Response Team. (2001b, 8 October 2001). UNIX Security Checklist v2.0 - The Essentials. Retrieved November 19, 2001, from http://www.auscert.org.au/Information/Auscert_info/Papers/usc20_essentials.html

Australian Computer Emergency Response Team (2004). *The Australian Computer Crime and Security Survey 2004.*

Avlonitis, M., Magkos, E., Stefanidakis, M., & Chrissikopoulos, V. (2007). A spatial stochastic model for worm propagation: scale effects. *Journal in Computer Virology, 3*(2), 87-92.

Aycock, J., deGraaf, R., & Jacobson, M. (2006). Anti-disassembly using cryptographic hash functions. *Journal in Computer Virology, 2*(1), 79-85.

Bace, B. (2000). Understanding Microsoft's October 26th Incident. Retrieved December 12, 2000, from http://www.tripwire.com/press/beckybaceWP.cfml

Bace, R., & Mell, P. (2001, November 2001). Intrusion Detection Systems. Retrieved March 23, 2002, from http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

Backhouse, J., & Dhillon, G. (1999). Working towards principles for information security management in the 21 st century. Retrieved Ocotber 17, 2001, from http://www.csrc.lse.ac.uk/ISSecurity.pdf

Baryamureeba, V., & Tushabe, F. (2004). *The Enhanced Digital Investigation Process Model*: Makerere University Institute of Computer Science, Uganda.

Bates, J. (1997). Fundamentals of Computer Forensics. *International Journal of Forensic Computing*(January/February 1997).

Bates, J. (1998). Forensic lessons - case study. *International Journal of Forensic Computing, 1998*(No 20), 16-19.

Bayer, U., Moser, A., Kruegel, C., & Kirda, E. (2006). Dynamic analysis of malicious code. *Journal in Computer Virology, 2*(1), 67-77.

. Bedworth Case - UK. (1993). Retrieved March 26, 2001, from http://www.eff.org/pub/Net_culture/Hackers/uk_court_acquits_teenage_hacker.article

Biskup, J., & Flegel, U. (2000a). On Pseudonymization of Audit Data for Intrusion Detection *Workshop on Design Issues in Anonymity and Unobservability* (Designing Privacy Enhancing Technologies ed., Vol. 2009, pp. 161-180). Berkeley, California: Springer-Verlag, Berlin, Heidelberg.

Biskup, J., & Flegel, U. (2000b). Threshold-Based Identity Recovery for Privacy Enhanced Applications *7th ACM Conference on Computer and Communications Security (CCS 2000)* (pp. 71-79). Athens, Greece: ACM.

Biskup, J., & Flegel, U. (2000c). Transaction-Based Pseudonyms in Audit-Data for Privacy Respecting Intrusion Detection *Third International Workshop on Recent Advances in Intrusion Detection (RAID 2000)* (Vol. 1907, pp. 28-48). Toulouse, France: Springer-Verlag, Berlin, Heidelberg.

Brenner, S. W., & Carrier, B. (2004). The Trojan Horse Defense in Cybercrime Cases. *Santa Clara Computer & High Technology Law Journal, 21*(1).

Broucek, V., Frings, S., & Turner, P. (2003). The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists. In C. Valli & M. Warren (Eds.), *1st Australian Computer, Network & Information Forensics Conference*. Perth, WA, Australia.

Broucek, V., & Turner, P. (2001a). Forensic Computing: Developing a Conceptual Approach for an Emerging Academic Discipline. In H. Armstrong (Ed.), *5th Australian Security Research Symposium* (pp. 55-68). Perth, Australia: School of Computer and Information Sciences, Faculty of Communications, Health and Science, Edith Cowan University, Western Australia.

Broucek, V., & Turner, P. (2001b). Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare. *Journal of Information Warfare, 1*(2), 95-108.

Broucek, V., & Turner, P. (2002a). Bridging the Divide: Rising Awareness of Forensic Issues amongst Systems Administrators *3rd International System Administration and Networking Conference*. Maastricht, The Netherlands.

Broucek, V., & Turner, P. (2002b). E-mail and WWW browsers: A Forensic Computing perspective on the need for improved user education for information systems security management. In M. Khosrow-Pour (Ed.), *2002 Information Resources Management Association International Conference* (pp. 931-932). Seattle Washington, USA: IDEA Group.

Broucek, V., & Turner, P. (2002c). Risks and Solutions to problems arising from illegal or Inappropriate On-line Behaviours: Two Core Debates within Forensic Computing. In U. E. Gattiker (Ed.), *EICAR Conference Best Paper Proceedings* (pp. 206-219). Berlin, Germany.

Broucek, V., & Turner, P. (2003a). A Forensic Computing perspective on the need for improved user education for information systems security management. In R. Azari (Ed.), *Current Security Management & Ethical Issues of Information Technology*. Hershey, PA 17033-1117, USA: IGP/INFOSCI/IRM Press.

Broucek, V., & Turner, P. (2003b, May 8-9). *Intrusion Detection Systems: Issues and Challenges in Evidence Acquisition.* Paper presented at the CTOSE Conference, Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium.

Broucek, V., & Turner, P. (2003c). Intrusion Detection: Forensic Computing Insights arising from a Case Study on SNORT. In U. E. Gattiker (Ed.),

EICAR Conference Best Paper Proceedings. Copenhagen, Denmark: EICAR.

Broucek, V., & Turner, P. (2004a). Computer Incident Investigations: e-forensic Insights on Evidence Acquisition. In U. E. Gattiker (Ed.), *EICAR Conference Best Paper Proceedings*. Luxembourg, Grand Duchy of Luxembourg: EICAR.

Broucek, V., & Turner, P. (2004b). Intrusion Detection: Issues and Challenges in Evidence Acquisition. *International Review of Law, Computers and Technology, 18*(2), 149-164.

Broucek, V., & Turner, P. (2005a). Considerations for e-forensics: Insights into Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-line Behaviours. *International Scientific Journal of Computing, 4*(2), 17-25.

Broucek, V., & Turner, P. (2005b). "Riding Furiously in All Directions" - Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-line Behaviours. In P. Turner & V. Broucek (Eds.), *EICAR 2005 Conference Best Paper Proceedings* (pp. 190-203). Saint Julians, Malta: EICAR.

Broucek, V., & Turner, P. (2006). Winning the Battles, Losing the War? Rethinking Methodology for Forensic Computing Research. *Journal in Computer Virology, 2*(1), 3-12.

Broucek, V., Turner, P., & Frings, S. (2005). Music piracy, universities and the Australian Federal Court: Issues for forensic computing specialists. *Computer Law & Security Report, 21*(1), 30-37.

Brungs, A., & Jamieson, R. (2005). Identification of Legal Issues for Computer Forensics. *Information Systems Management, 22*(2), 57 - 66. doi: 10.1201/1078/45099.22.2.20050301/87278.7

Burrell, G., & Morgan, G. (1985). *Sociological Paradigms and Organizational Analysis*. Portsmouth: Heinemann Educational Books.

Carney, M., & Rogers, M. (2004). The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction. *International Journal of Digital Evidence, 2*(4).

Carrier, B. D., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence, 2*(2).

Carvalho, M., Ford, R., Allen, W., & Marin, G. (2008). Securing MANETs with BITSI: danger theory and mission continuity. In B. V. Dasarathy (Ed.), *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008* Orlando, FL, USA: SPIE.

Casey, E. (2000). *Digital Evidence and Computer Crime*: Academic Press.

Castells, M. (2000). *The Rise of The Network Society: The Information Age: Economy, Society and Culture* (2 ed. Vol. 1).

Chess, D. M., & White, S. R. (2000). *An undetectable computer virus*. Paper presented at the Virus Bulletin Conference.

Chisum, W. J. (1999). An introduction to crime reconstruction. In B. Turvey (Ed.), *Criminal Profiling: An Introduction to Behavioural Evidence Analysis*. London: Academic Press.

Christy, J. (1998). Rome Laboratory Attacks: Prepared Testimony of Jim Christy, Air Force Investigator, before the Senate Governmental Affairs Committee, Permanent Investigation Subcommittee, May 22, 1996. In D. E. Denning & P. J. Denning (Eds.), *Internet Besieged: Countering Cyberspace Scofflaws* (pp. 57-65): ACM Press.

Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigation. *International Journal of Digital Evidence, 3*(1).

Clayton, R. (2000). The Limits of Traceability. Retrieved 10 December, 2002, from http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.pdf

Cohen, F. (1986). *Computer Viruses.* PhD thesis, University of Southern California.

Coles-Kemp, L., & Overill, R. E. (2007). On the role of the Facilitator in information security risk assessment. *Journal in Computer Virology, 3*(2), 143-148.

Commission of European Communities (2005). *Green Paper on European Programme for Critical Infrastructure Protection.* Brussels: Commission of European Communities.

Commission of European Communities. (2009). *Protecting Critical Information Infrastructures: Frequently Asked Questions*. Brussels: Commission of European Communities Retrieved from http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/141&format=PDF&aged=0&language=EN&guiLanguage=en.

Council of Europe. (2001). *Convention on Cybercrime.* Budapest: Council of Europe.

CTOSE (2003). *CTOSE Project Final Results.*

Cybersecurity Act of 2009, The Senate of the United States (2009).

Denning, D. E. (1997, 26 February 1997). Description of Key Escrow System. Retrieved 16 March 2001, 2001, from http://www.cosc.georgetown.edu/~denning/crypto/Appendix.html

Denning, D. E. (1999). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Retrieved January 13, 2001, from http://www.nautilus.org/info-policy/workshop/papers/denning.html

Denning, D. E., & Branstad, D. K. (1996). A Taxonomy for Key Escrow Encryption Systems. *Communications of the ACM, 39*(3).

Department of Foreign Affairs and Trade. (1997). *Treaty between the Government of Australia and the Government of United States of America on Mutual Assistance in Criminal Matters, and Exchange of Notes*. Washington.

Desai, N. (2002). Increasing Performance in High Speed NIDS: A look at Snort's Internals. Retrieved March 13, 2002, from http://www.snort.org/docs/Increasing_Performance_in_High_Speed_NIDS.pdf

Dishaw, M. T. (2002). Monitoring Internet Use In the Workplace: Caution is Advised. In M. Khosrow-Pour (Ed.), *2002 Information Resources Management Association International Conference* (pp. 175-178). Seattle, WA, USA: Idea Group Publishing.

. ethereal (Version 0.9.7). (2002). Retrieved from http://www.ethereal.com

Etter, B. (2000a). The Challenges of E-Crime for Australasian Law Enforcement. Retrieved November 14, 2001, from http://www.acpr.gov.au/pdf/Presentations/pmdpdec.pdf

Etter, B. (2000b). Evaluating the Capacity to Respond to E-Crime. Retrieved November 14, 2001, from http://www.acpr.gov.au/pdf/Presentations/Nat_Sympos.pdf

Etter, B. (2000c). Working in Partnership: The Australasian Response to Electronic Crime. Retrieved November 14, 2001, from http://www.acpr.gov.au/pdf/Presentations/ccrime.pdf

Etter, B. (2001). The Forensic Challenges of E-Crime. Retrieved November 14, 2001, from http://www.acpr.gov.au/pdf/Presentations/forchall.pdf

European Commission, D.-G. f. e., industrial relations and social affairs, Unit V/B/4 (1997). *Building the European Information Society for us all.* Brussells: European Commission.

European Parliament, & Council of the European Union. (2002). Directive 2002/58/EC - Directive on Privacy and Electronic Communication. *Official Journal of the European Communities, L*(201), 37-47.

Even, L. R. (2000). What is a Honeypot? Retrieved March 20, 2003, from http://www.sans.org/newlook/resources/IDFAQ/honeypot3.htm

Farmer, D. (2000). What are MACtimes? Powerful tools for digital databases. *Dr Dobb's Journal, 29*(10).

Farmer, D. (2001). Bring Out Your Dead. The Ins and Outs of Data Recovery. *Dr Dobb's Journal, 30*(1).

Farmer, D., & Venema, W. (1993). Improving the Security of Your Site by Breaking Into it. Retrieved January 12, 2001, from http://www.fish.com/security/admin-guide-to-cracking.html

Farmer, D., & Venema, W. (1999). Murder on the Internet Express. Retrieved November 6, 2001, from http://www.fish.com/forensics/class.html

Farmer, D., & Venema, W. (2000). Forensic Computer Analysis: an Introduction. Reconstructing Past Events. *Dr Dobb's Journal, 29*(9), 70-75.

Filiol, E. (2006a). Malware pattern scanning schemes secure against black-box analysis. *Journal in Computer Virology, 2*(1), 35-50.

Filiol, E. (2006b). [Personal communication: e-mail].

Filiol, E. (2007). Formalisation and implementation aspects of K-ary (malicious) codes. *Journal in Computer Virology, 3*(2), 75-86.

Filiol, E., & Josse, S. (2007). A statistical model for undecidable viral detection. *Journal in Computer Virology, 3*(2), 65-74.

Ford, R. (2008). [Personal communication: e-mail questionnaire].

Frings, S. (2006). *Method for the structured documentation of IT incident management.* Paper presented at the ECCE 2006, E-crime and computer evidence, Nottingham.

Frings, S., Stanisic-Petrovic, M., & Urry, R. (2003). Holistic Approach for Processing Electronic Evidence Related to High-Tech Crime and Severe Disputed Electronic Transactions: Cyber Crime Advisory Tool - C*CAT. In U. E. Gattiker (Ed.), *EICAR 2003 Conference Best Paper Proceedings*. Copenhagen, Denmark: EICAR.

Galliers, R. (1992). Choosing information systems research approach. In R. Galliers (Ed.), *Information Systems Research: Issues, Methods and Practical Guidelines.* Oxford: Blackwell Scientific Publications.

Gattiker, U. E. (2007). Bologna process revisited: educating information security and malware experts. *Journal in Computer Virology, 3*(2), 149-161.

Geiger, M. (2005). *Evaluating Commercial Counter-Forensic Tools*. Paper presented at the Digital Forensic Research Workshop (DFRWS), New Orleans, LA.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20.

Haagman, D., & Ghavalas, B. (2005a). Trojan Defence: A Forensic View. *Digital Investigation, 2*(1), 23-30.

Haagman, D., & Ghavalas, B. (2005b). Trojan Defence: A Forensic View Part II. *Digital Investigation, 2*(2), 133-136.

Handley, M., Paxson, V., & Kreibich, C. (2001). Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics *10th USENIX Security Symposium*. Washington, DC, USA.

Hanks, P. (Ed.). (1991). *The Collins Australian pocket Dictionary of the English Language*: HarperCollins Publishers.

Hannan, M., Frings, S., Broucek, V., & Turner, P. (2003). Forensic Computing Theory & Practice: Towards developing a methodology for a standardised approach to Computer misuse. In S.-A. Kinght (Ed.), *1st Australian Computer, Network & Information Forensics Conference*. Perth, WA, Australia.

Hannan, M., & Turner, P. (2004, 28-29 June). *The Last Mile: Applying Traditional Methods for Perpetrator Identification in Forensic Computing Investigations*. Paper presented at the 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London.

Hannan, M., Turner, P., & Broucek, V. (2003). Refining the Taxonomy of Forensic Computing in the Era of E-crime: Insights from a Survey of Australian Forensic Computing Investigation (FCI) Teams. *4th Australian Information Warfare and IT Security Conference* (pp. 151-158). Adelaide, SA, Australia.

Heller, M. (2008). *The Gridlock Economy: How Too Much Ownership Wrecks Markets, Stops Innovation, and Costs Lives* Basic Books.

Internet Freedom Preservation Act, The Senate of the United States (2009).

Jorns, O., Jung, O., & Quirchmayr, G. (2007). Transaction pseudonyms in mobile environments. *Journal in Computer Virology, 3*(2), 185-194.

Josse, S. (2006). How to asses the effectiveness of your anti-virus? *Journal in Computer Virology, 2*(1), 51-65.

Josse, S. (2007). Rootkit detection from outside the Matrix. *Journal in Computer Virology, 3*(2), 113-123.

Kayayurt, B., & Tuglular, T. (2006). End-to-end security implementation for mobile devices using TLS protocol. *Journal in Computer Virology, 2*(1), 87-97.

Kelman, A. (1999). Computer Crime in the 1990s, A Barrister's View. Retrieved December 1, 2000, from http://www.csrc.lse.ac.uk/ComputerCrime1990s.htm

Kim-Kwang, R. C. (2009). *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences.* Canberra: Australian Institute of Criminology.

Klensin, J. (2001). RFC2821 - Simple Mail Transfer Protocol. Retrieved December 12, 2001, from http://www.ietf.org/rfc/rfc2821.txt?number=2821

Kruegel, C., & Toth, T. (2003). Automatic Rule Clustering for improved, signature based Intrusion Detection. Retrieved January 16, 2003, from http://www.infosys.tuwien.ac.at/snort-ng/snort-ng.pdf

Kvarnström, H., Lundin, E., & Jonsson, E. (2000). Combining fraud and intrusion detection - meeting new requirements *The fifth Nordic Workshop on Secure IT systems (NordSec2000).* Reykjavik, Iceland.

Laing, B. (2000). How To Guide: Impletmenting a Network Based Intrusion Detection System. Retrieved November 21, 2001, from http://www.snort.org/docs/iss-placement.pdf

Lamount, L. (2003). Recording firms ask to scan university computers. Retrieved February 19, 2003, from http://www.smh.com.au/articles/2003/02/18/105330603596.html

Leroux, O., & Pérez Asinari, M. V. (2003, May 8-9). *Collecting and Producing Electronic Evidence in Cybercrime Cases.* Paper presented at the CTOSE Conference, Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium.

Leyden, J. (2000). Microsoft hacked in Balkans. U.S. Companies' overseas web sites are dropping like flies. Retrieved December 17, 2000, from http://www.securityfocus.com/news/125

Li, L., & Helenius, M. (2007). Usability evaluation of anti-phishing toolbars. *Journal in Computer Virology, 3*(2), 163-184.

Liu, V., & Brown, F. (2006). *Bleeding-Edge Anti-Forensics*. Paper presented at the Infosec Worl Conference and Expo.

Lundin, E. (2000). Anomaly-based intrusion detection: privacy concerns and other problems. *Computer Networks, 34*(4), 623-640.

Lundin, E., & Jonsson, E. (1999a). Privacy vs Intrusion Detection Analysis *The 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99)*. Lafayette, Indiana, USA.

Lundin, E., & Jonsson, E. (1999b). Some Practical and Fundamental Problems with Anomaly Detection *The fourth Nordic Workshop on Secure IT systems (NORDSEC'99)*. Kista, Sweden.

Maher, W. (2001, January 2001). Learning from the Microsoft Crack. *Australian Personal Computer, 22,* 114-115.

McCullagh, A., & Caelli, W. (2003). Extended case note and commentary: Sony Music Entertainment (Australia) Limited & others v. University of Tasmania & others [2003] FCA 532 (30 May 2003). *The Computers and Law Journal, September 2003*(53).

McKemmish, R. (1999). What is Forensic Computing. *Trends and Issues in Crime and Criminal Justice*(118).

Mell, P., Marks, D., & McLarnon, M. (2000). A denial-of-service resistant intrusion detection architecture. *Computer Networks, 34*, 641-658.

Microsoft (2000). *Microsoft Responds to Security Issue* (Press release). Redmond: Microsoft.

. Microsoft UK website Hacked - VIGILANTe Statement. (2001). Retrieved May 8, 2001, from http://www.itsecurity.com/tecsnews/may2001/may55.htm

Mitchison, N. (2009). [Personal communication: e-mail].

Mitnick, K. (2000). Microsoft hack wasn't espionage. Retrieved November 7, 2000, from http://www.securityfocus.com/news/112

. mod_ssl (Version 2.8.10). (2002). Retrieved from http://www.modssl.org/

Morgan, A. (2003). It's war on a generation of cyber pirates. Retrieved February 18, 2003, from http://www.smh.com.au/articles/2003/02/17/105330539310.html

Myers, J., & Rose, M. (1996). RFC1939 - Post Office Protocol - Version 3. Retrieved July 14, 2002, from http://www.ietf.org/rfc/rfc1939.txt?number=1939

National High-Tech Crime Unit, & Association of Cheif Police Officers. (2003). *Good Practice Guide for Computer based Electronic Evidence.*

Nelson, D. (2003a, August 5). Protecting intellectual property, *The Age,* p. Next 3.

Nelson, D. (2003b, August 5). Student piracy row may leave IT to face the music, *The Age,* p. Next 3.

Neuman, W. L. (2000). *Social Research Methods: Qualitative and Quantitative Approaches* (4th ed.). Boston: Allyn and Bacon.

Ondi, A., & Ford, R. (2007). How good is good enough? Metrics for worm/anti-worm evaluation. *Journal in Computer Virology, 3*(2), 93-101.

. Online piracy hurts 2002 music sales: ARIA. (2003). Retrieved January 24, 2003, from http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20271487,00.htm

. openssl (Version 0.9.6g). (2002). Retrieved from http://www.openssl.org/

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organisations: research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.

Palmer, G. (2001). *A Road Map for Digital Forensic Research: Report From the First Digital Forensic Research Workshop (DFRWS)* (DFRWS Technical Report No. DTR-T001-01 Final). Utica, New York: DFRWS.

Patel, A., & Ciardhuáin, S. Ó. (2000, November 2000). The Impact of Forensic Computing on Telecommunications. *IEEE Communications Magazine,* 64-67.

Pearce, J. (2003). Evidence of piracy allegedly destroyed. Retrieved July 25, 2003, from http://news.zdnet.co.uk/business/0,39020645,2138165,00.htm

Postel, J. B. (1982). RFC821 - Simple Mail Transfer Protocol. Retrieved December 12, 2001, from http://www.ietf.org/rfc/rfc0821.txt?number=821

Poulsen, K. (2000). When Microsoft Kicked a hacker off its network, the FBI may have lost its chance for a bust. Retrieved November 1, 2000, from http://www.securityfocus.com/news/109

Preuß, J., Furnel, S. M., & Papadaki, M. (2007). Considering the potential of criminal profiling to combat hacking. *Journal in Computer Virology, 3*(2), 135-141.

Ptacek, T. H., & Newsham, T. N. (1998). Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. Retrieved November 11, 2001, from http://www.snort.org/docs/idspaper/

Rathmell, A., & Valeri, L. (2003). *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence, 1*(3).

Reno, J. (1996). Law Enforcement in Cyberspace Address. In D. E. Denning & P. J. Denning (Eds.), *Internet Besieged: Countering Cyberspace Scofflaws* (pp. 439-447): ACM Press.

Richta, R. (1977). The Scientific and Technological Revolution and the Prospects of Social Development. In R. Dahrendorf (Ed.), *Scientific-Technological Revolution. Social Aspects.* (pp. 25-72). London: Sage.

Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks *13th Systems Administration Conference - LISA '99.* Seattle, WA.

Roesch, M. (2001a). Snort 1.8.7 [man pages].

Roesch, M. (2001b, July 4, 2002). Snort Users Manual - Snort Release: 1.8.7. Retrieved July 27, 2002, from http://www.snort.org

Rohde, L. (2000). Bulletin: Microsoft stung by hack attack. Retrieved January 26, 2001, from http://www.computerworld.com/cwi/story/0,1199,NAV47_STO52929,00.html

Rose, D. (2003, August 2). Uni hit by Net piracy action, *The Saturday Mercury,* p. 13.

Samuelson, P. (2002). Toward a "New Deal" for Copyright in the Information Age. [Digital Copyright by Jessica Litman]. *Michigan Law Review, 100*(6), 1488-1505.

Sato, O., Broucek, V., & Turner, P. (2005). Electronic Evidence Management for Computer Incident Investigations: A Prospect of CTOSE. *Security Management, 18*(3), 11-18.

Scientific Working Group on Digital Evidence (SWGDE), & International Organization on Computer Evidence (IOCE). (2002). Digital Evidence: Standards and Principles. *Forensic Science Communications, 2*(2).

Shimomura, T. (1995). Takedown: the Mitnick Case. from http://www.takedown.com/

Sliwa, C. (2000). Users show some sympathy to Microsoft over security breach. Retrieved November 07, 2000, from http://www.computerworld.com/cwi/story/0,1199,NAV47_STO53471,00.html

Smith, D., & Indulska, J. (2001). Enhancing Security of Unix Systems. Retrieved November 17, 2001, from http://www.auscert.org.au/Information/Auscert_info/Papers/Enhancing_Security_of_Unix_Systems.html

Sobirey, M., Fischer-Hübner, S., & Rannenberg, K. (1997). Pseudonymous audit for privacy enhanced intrusion detection. In L. Yngstrom & J. Carlsen (Eds.), *IFIP TC11 13th International Conference on Information Security (SEC'97)* (pp. 151-163). Copenhagen, Denmark: Chapman & Hall, London, UK.

Sommer, P. (1998a). Digital Footprints: Assessing Computer Evidence. *Criminal Law Review Special Edition*, 61-78.

Sommer, P. (1998b). Intrusion Detection Systems as Evidence *Recent Advances in Intrusion Detection - RAID'98*. Louvain-la-Neuve, Belgium.

Sommer, P. (1999). Intrusion Detection Systems as Evidence. *Computer Networks, 31*(23-24), 2477-2487.

Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 532 (30 May 2003) (Federal Court of Australia 2003).

Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 724 (18 July 2003) (Federal Court of Australia 2003).

Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 805 (29 July 2003) (Federal Court of Australia 2003).

Sony Music Entertainment (Australia) Limited v University of Tasmania [2003] FCA 929 (4 September 2003) (Federal Court of Australia 2003).

Cyber Security - How Can We Protect American Computer Networks From Attack?, House Science Committee on InfoSec Sess. (2001).

Spitzner, L., & Roesch, M. (2001a, 10 October 2001). The Value of Honeypots, Part One: Definitions and Values of Honeypots. Retrieved November 1, 2001, from http://www.securityfocus.com/cgi-bin/infocus.pl?id=1492

Spitzner, L., & Roesch, M. (2001b, 23 October 2001). The Value of Honeypots, Part Two. Retrieved November 1, 2001, from http://www.securityfocus.com/cgi-bin/infocus.pl?id=1498

. ssh (Version 3.2). (2002). Retrieved from http://www.ssh.com/solutions/secureshell.html

Stephenson, P. R. (2000a). The Application of Intrusion Detection Systems in a Forensic Environment *Recent Advances in Intrusion Detection - RAID 2000*. Toulouse, France.

Stephenson, P. R. (2000b). Intrusion Management: A Top Level Model for Securing Information Assets in an Enterprise Environment. In U. E. Gattiker (Ed.), *EICAR 2000* (pp. 287-298).

Stoll, C. (1988). Stalking the Wily Hacker. *Communications of the ACM, 31*(5), 484-497.

Stoll, C. (1989). *The Cuckoo's Egg*: Doubleday.

. tcpdump/libpcap (Version 3.7.1). (2002). Retrieved from http://www.tcpdump.org/

ten Houten, J. (2007a). *Fraud Investigation and Forensic Computing.* Paper presented at the Digital Forensic Forum, Prague 2007, Prague.

ten Houten, J. (2007b). [Personnal Communication: interview/discussion].

Touraine, A. (1988). *Return of the Actor.* Minneapolis: University of Minnesota Press.

Tripp, G. (2006). A parallel "String Matching Engine" for use in high speed network intrusion detection system. *Journal in Computer Virology, 2*(1), 21-34.

Tripp, G. (2007). Regular expression matching with input compression: a hardware design for use within network intrusion detection systems. *Journal in Computer Virology, 3*(2), 125-134.

U.S. Secret Service, IACP, & DOJ. (2006). *Best Practices for Seizing Electronic Evidence V2.* Retrieved from http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/downloads/other/bestpractices.pdf/view.

Urry, R., & Mitchison, N. (2003, May 8-9). *CTOSE Project. Electronic Evidence: gathering, securing, integrating, presenting.* Paper presented at the CTOSE Conference, Facultés Universitaires Notre-Dame De la Paix, Namur, Belgium.

Venema, W. (1992). TCP WRAPPER: Network monitoring, access control, and booby traps. *3rd UNIX Security Symposium.* Baltimore, USA.

Venema, W. (2000a). File Recovery Techniques. Files Wanted, Dead or Alive. *Dr Dobb's Journal, 29*(12).

Venema, W. (2000b, December 12). [Personal Communication: e-mail].

Venema, W. (2000c). Strangers in the Night. Finding the Purpose of an Unknown Program. *Dr Dobb's Journal, 29*(11).

Verton, D. (2000). Think tank warns that Microsoft hack could pose national security risk. Retrieved January 5, 2001, from http://www.computerworld.com/cwi/story/0,1199,NAV47_STO55656,00.html

Vinoo, T., & Nitin, J. (2007). Bot countermeasures. *Journal in Computer Virology, 3*(2), 103-111.

Webster, F. (1997). *The Theories of Information Societies*. London: Routledge.

Weiss, T. R., & Rosencrance, L. (2000). Update: Microsoft stung by hack attack. Retrieved October 28, 2000, from http://www.computerworld.com/cwi/story/0,1199,NAV47_STO52949,00.html

Wu, T. (2003). Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law, 2*(2).

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer Forensics Education. *IEEE Security & Privacy, 1*(4), 15-23.

Yin, R. K. (1994). *Case Study Research: Design and Methods.* (2nd ed.). Thousands Oaks, CA: Sage.

Yuill, J., Wu, S. F., Gong, F., & Huang, M.-Y. (1999). Intrusion Detection for an On-Going Attack *Recent Advances in Intrusion Detection - RAID'99.* Purdue, IN, USA.

Zimmerman, P. (1996). Testimony of Philip R. Zimmerman to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation. Retrieved 20 March 2001, 2001, from http://web.mit.edu/prz/testimony.shtml

Zimmerman, P. (2001). A note to PGP users. Retrieved 22 February 2001, 2001, from http://web.mit.edu/prz/text/PRZ_leaves_NAI.txt

Zittrain, J. L. (2008). *The Future of the Internet And How to Stop It.* New Heaven & London: Yale University Press.

Appendix

This section contains selected papers as published in academic journals and peer reviewed conference proceedings. These are:

Broucek, V., & Turner, P. (2001). Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare. *Journal of Information Warfare, 1*(2), 95-108. **This paper has been awarded the "Best General Article 2002" award by the National Institute of Forensic Science, Australia.**

Broucek, V., & Turner, P. (2002). Bridging the Divide: Rising Awareness of Forensic Issues amongst Systems Administrators *3rd International System Administration and Networking Conference*. Maastricht, The Netherlands.

Broucek, V., & Turner, P. (2002). Risks and Solutions to problems arising from illegal or Inappropriate On-line Behaviours: Two Core Debates within Forensic Computing. In U. E. Gattiker (Ed.), *EICAR Conference Best Paper Proceedings* (pp. 206-219). Berlin, Germany: EICAR.

Broucek, V., Frings, S., & Turner, P. (2003). The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists. In C. Valli & M. Warren (Eds.), *1st Australian Computer, Network & Information Forensics Conference*. Perth, WA, Australia. **This paper has been awarded the "Best Student Paper" award.**

Broucek, V., & Turner, P. (2003). A Forensic Computing perspective on the need for improved user education for information systems security management. In R. Azari (Ed.), *Current Security Management & Ethical Issues of Information Technology*. Hershey, PA 17033-1117, USA: IGP/INFOSCI/IRM Press.

Broucek, V., & Turner, P. (2004). Intrusion Detection: Issues and Challenges in Evidence Acquisition. *International Review of Law, Computers and Technology, 18*(2), 149-164.

Broucek, V., & Turner, P. (2005). "Riding Furiously in All Directions" - Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-line Behaviours. In P. Turner & V. Broucek (Eds.), *EICAR 2005 Conference Best Paper Proceedings* (pp. 190-203). Saint Julians, Malta: EICAR.

Broucek, V., & Turner, P. (2005). Considerations for e-forensics: Insights into Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-line Behaviours. *International Scientific Journal of Computing, 4*(2), 17-25.

Broucek, V., Turner, P., & Frings, S. (2005). Music piracy, universities and the Australian Federal Court: Issues for forensic computing specialists. *Computer Law & Security Report, 21*(1), 30-37.

Broucek, V., & Turner, P. (2006). Winning the Battles, Losing the War? Rethinking Methodology for Forensic Computing Research. *Journal in Computer Virology, 2*(1), 3-12.

¢KŜ l·LJLJŜyŘƛǑŜă fƛăűŜŘ l·ō2ØŜ Kl·ØŜ ōŜŜyNJSY2ØŜŘ ŦƧNJ Ǒ2LJèNJƛƎKű ƧNJ LJNJ2LJNJƛŜűl·NJè NJŜasons.